D1.2.2

Cloud Computing: Legal Analysis

Project number:	257243
Project acronym:	TClouds
Project title:	Trustworthy Clouds - Privacy and Resilience for Internet-scale Critical Infrastructure
Start date of the project:	1st October, 2010
Duration:	36 months
Programme:	FP7 IP

Deliverable type:	Report
Deliverable reference number:	ICT-257243 / D1.2.2/ 1.0
Activity and Work package contributing to the deliverable:	Activity 1 / WP 1.2
Due date:	September 2011 – M12
Actual submission date:	3rd October, 2011

Responsible organisation:	ULD
Editor:	Ninja Marnau, Eva Schlehahn
Dissemination level:	Public
Revision:	1.0

Abstract:	D1.2.2 identifies critical issues of cloud computing with respect to the current European data protection legislation. The legal foundations of European privacy & data protection and their basic principles will be presented, focusing mainly on the requirements of the EU Data Protection Directive 95/46/EC. The provisions of accountability of data processors and controllers will be explained and the conditions under which lawful data processing can take place will be analysed. The additional challenges of cross-border data transfers in a cloud environment will be discussed. Finally, this deliverable highlights possible resolutions and draws conclusions by forecasting future legal challenges of cloud computing.
Keywords:	Cloud computing, data protection, privacy, personal data, EU-Law, EU Data Protection Directive 95/46/EC, Data controller, Data processor, E-Privacy and data retention directives, Safe Harbor, EU Standard Contract Clauses, Binding Corporate Rules

Editor

Ninja Marnau, Eva Schlehahn (ULD)

Contributors

Ninja Marnau, Eva Schlehahn (ULD)

Disclaimer

This work was partially supported by the European Commission through the FP7-ICT program under project TClouds, number 257243.

Executive Summary

This deliverable will identify the key issues related to cloud computing and European data protection legislation. The scope of research comprises determining the legal foundation of privacy & data protection and their basic principles. Though tackling the applicability of the EU E-Privacy Directive 2002/58/EC, it's related Directives, the EU Data Retention Directive 2006/24/EC and the national law of the EU member states, this document thereby mainly focuses on the legal requirements provisioned by the EU Data Protection Directive 95/46/EC. Mandatory realisation requirements will be identified, such as the legal responsibility of involved parties, grounded on a clear differentiation of the roles of data processors and controllers. It then approaches the most critical issues specifically in the cloud computing field in respect to data protection and privacy.

In this context, this document will address legal issues like applicable law, the loss of the immediate control over the data and the potential access of third parties. Also, the sector-specific difficulties of legal responsibility allocation in the cloud computing context will be addressed. This also comprises the additional intricacies of cross-border transmissions of personal data and the transnational enforcement of European citizen's data protection rights. Within this context, the EU-US Safe Harbor agreement will be analysed in-depth and assessed in respect to its suitability to ensure the protection of personal data disclosed from the European domain.

We will draw the proximate consequences and present potential methods of resolution in regard to cloud computing. These methods encompass legal approaches, such as first steps mandatory for the assignment of legal responsibilities and the assertion of legislative requirements. Furthermore, contractual and other possible regulations, respectively the EU Standard Contractual Clauses, Codes of Conduct and Binding Corporate Rules will be introduced and evaluated in respect to their applicability in cloud computing scenarios. Moreover, the impact of audits and certifications as well as of technical solutions, e.g. standardisation efforts and Privacy by Design approaches will be scrutinised.

Finally, we will make general conclusions and do a forecast to the challenges of cloud computing faced with the exigencies of legal and technical compliance resulting of the current European data protection legislation.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

Cloud Computing is at the heart of a long-lasting hype. While IT experts still discuss the universal definition of this term, more and more providers of services aim at positioning themselves on the rapidly growing market. Multitude usage possibilities are being offered via networks like the Internet, cost-efficiently as so-called pay-as-you-go services tailored to the customers' needs. However, the processing of personal and critical business data in a cloud, on foreign servers, arises serious privacy and data security concerns. Consequently, these concerns are hurdles yet to overcome to enable a full exploitation of the various cloud computing business models.

The TClouds project aims at developing a trustworthy cloud computing system, which makes the lawful processing of critical infrastructures in cloud computing possible. A main focus of research will be the creation of a secure cloud-of-clouds environment, which is compliant with the European data protection requirements. This shall be possible without dispensing the advantages of cloud computing, such as scalability and availability of offered services and saving of expenses. Furthermore, new and open security standards as well as more effective cloud-management components shall be developed. Hitherto existing cloud systems convey the handicap that customers of services do not know where their data is stored and how exactly it will be processed. This entails a grievous loss of control for the potential subscriber of cloud services. Furthermore, especially in cases of cross-border data transfers in and outside the European Union, respectively the European Economic Area, numerous legal issues arise with respect to the protection of personal data and sensitive information. This entails first basic, yet essential questions like jurisdiction and enforcement of legal requirements. In this context, already the potential multitude of different vendors and users of cloud computing services may render the appropriate allocation of data protection related obligations and their corresponding legal responsibilities extremely difficult. This is one of the main focus points of this document, whereas the identification of involved parties and their classification into unequivocal roles is a mandatory procedure to enable the protection of any individual's personal data. It is an essential precondition for the accountability of data collecting, storing and processing entities not just of legal, but within any kind of enforcement actions. Furthermore, the lack of milestone court decisions leads to a number of legal uncertainties, which we seek to resolve by presenting and analysing more possible methods of resolution. It will be the challenge for future and in particular for the further progress of this project, to encounter these difficulties and research both legal and technical ways to make cloud computing fit for the everyday utilisation of personal data compliant with the European data protection law. This is a first edition of D1.2.2 - Cloud Computing: Legal Analysis. Due to the latest valid version of the European data protection framework currently undergoing revision, we will closely watch the legislative, political and judicial processes and adapt this document with regard to these.

Chapter 2

The legal foundation of privacy and data protection

This section will introduce the legal framework that is relevant in terms of privacy and data protection. It will present the high level requirements on European level as well as an insight into the relationship with the national law of the EU member states. This section will be followed by the more precise and case relevant requirements being presented in Section 2.2 (Realisation requirements). Then, the breakdown and application of these requirements to the circumstantial cloud computing situation will be addressed later in the cloud-scenario-specific analysis in Section 2.3. (Critical factors for data protection in cloud computing).

2.1 General Provisions

The term "Privacy" is one of the most complex in the field of law and policy. Numerous definitions and understandings of this term exist, beginning with the discussion whether privacy is to be considered a condition, an interest, a claim, a (human) right or a mere social life concept. What many of the different views on privacy have in common is that is understood as some kind of protection against external influence on the personal space. So Schoeman considers privacy in principle as a protection against overreaching social control by others through their access to information or their control over decision making (1992).[1] Similarly, Bloustein stated that privacy is protection against personality, independence, dignity and integrity violations.[2] Robert Ellis Smith, editor of the Privacy Journal, focuses on the flip side of the coin and refers to specific means of privacy violation, such as interruption, intrusion, embarrassment, accountability and the attempt of unauthorised control over the if, when and how of information disclosure.[3] Likewise, DeCew sees privacy as a shield against scrutiny, prejudice, pressure to conform, exploitation and the judgement of others.[4]

For a comprehensive definition of the term "privacy", Clarke stated that privacy has several dimensions[5], such as:

[1] Schoeman, F., (ed.), 1984, *Philosophical Dimensions of Privacy: An Anthology*, Cambridge: Cambridge University Press.

[2] Edward Bloustein, *Privacy as an Aspect of Human Dignity*, 39 New York University Law Review 971 (1964).

[3] Robert Ellis Smith, Ben Franklin's Web Site 6 (Sheridan Books 2000).

[4] DeCew, Judith, *Privacy*, The Stanford Encyclopaedia of Philosophy (Fall 2008 Edition), Edward N. Zalta (ed.), URL = http://plato.stanford.edu/archives/fall2008/entries/privacy/.

[5] Roger Clarke, *Introduction to Dataveillance and Information Privacy, and Definitions of Terms,* original of 15 August 1997, latest revs. 16 September 1999, 8 December 2005, 7 August 2006 http://www.rogerclarke.com/DV/Intro.html#Priv.

- Privacy of the person (bodily privacy)
- Privacy of personal behaviour (such as sexual preferences, habits, political activities and religious practices)
- Privacy of personal communications (interaction with other persons or organisations) and
- Privacy of personal data (control of an individual over his/her data and its use)

Another approach would be to assume Bygrave's four principal ways to define privacy[6], such as

- non-interference
- limited accessibility
- privacy as information control and
- a mix of the aforementioned, linked exclusively to intimate or sensitive aspects of person's lives

Besides these specific approaches mentioned above, privacy is often understood mostly as a matter of fairness. This applies especially for the perception of privacy in the U.S.A. It comprises a main focus on privacy as an expression of self-realisation of the individual, derived as a characteristic of the constitutionally guaranteed pursuit of happiness. This also means that privacy is seen as a concept that is in itself per se opposed to interests of society. As a consequence, it is always subjected to a consideration process, in which it is predominantly considered as a right defeasible for an adequate price or intention. The perspective of the European countries is somewhat different, basically with a broader scope in respect to historic experiences of totalitarian regimes and understands privacy also as expedient for societal needs.[7] Already John Locke emphasised that human rights and individual freedom have particular significance in European countries as a result of their historical development.[8] Consequently, privacy must be seen as a human right to sustain the personal freedom of an individual in society and functions as a protection mechanism against knowledge, disclosure, interference or invasion by governments, companies or fellow citizens. However, in this function it is not only a defence right, but also serves as protective mechanism for the principles of a free democratic basic order. It is also not generally opposed to the interests of society.

Also, a differentiation has to be made between privacy and the concept of information control. In Europe, information control is not always directly linked to privacy.[9] So for example, the principle of the German informational self-determination (informationelle Selbstbestimmung) is a constitutional right in itself, which is derived from the 1983 census landmark decision[10] of the German Federal Constitutional Court.[11]

---

[6] Lee A. Bygrave, *Privacy Protection in a Global Context – A Comparative Overview*, 2004.

[7] For a more complex and in-depth examination of the historical development of the European Union, see Desmond Dinan, *Ever Closer Union: An Introduction to European Integration* (fourth edition), 2010.

[8] John Locke, *Two treatises of government*, Book II, Chapter II. Sect. 4 and 6.

[9] For the conjunction between the definitions of privacy and identity, see Kai Rannenberg, Denis Royer, André Deuker (ed.), *The Future of Identity in Information Society - Challenges and Opportunities*, pp. 292 ff. (section 7.3 When Idem meets Ipse: The Identity of the European Citizen).

[10] Volkszählungsurteil Bundesverfassungsgericht vom 15. Dezember 1983.

To safeguard privacy, the raw concept must be accompanied by tangible rights, which are not defeasible. In the legal field, the objectives of privacy can be stated as rather abstract cornerstones, such as the respect for private and family life in Article 8 European Convention on the Protection of Human Rights and fundamental Freedoms. Furthermore, Article 8 of the Charter of Fundamental Rights of the European Union (2000/C 364/01) refers explicitly to the protection of personal data:

1. *Everyone has the right to the protection of personal data concerning him or her.*
2. *Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.*
3. *Compliance with these rules shall be subject to control by an independent authority.*

The Treaty on the functioning of the European Union (hereinafter: TFEU) states in its consolidated version in Article 16 (ex Article 286 TEC) that

1. *Everyone has the right to the protection of personal data concerning them.*
2. *The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities. The rules adopted on the basis of this Article shall be without prejudice to the specific rules laid down in Article 39 of the Treaty on European Union.*

To guarantee an effective protection, privacy must get further refined in specific rights for concerned individuals, such as tangible data subject's rights to get informed about the collection and use of data elated to him/her, have access to that data, demand the alteration or deletion of this data and object the collection of data in the first place. Also, the parties involved and their obligations as well as their legal responsibilities must be determined.

For the European Union and European Community, respective the European Economic Area, such rights are laid down in the following frameworks:

- 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 (hereinafter referred to as: EU Data Protection Directive 95/46/EC)
- Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC (hereinafter referred to as: E-Privacy Directive) concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws

[11] Cf. the Canadian concept of informational self-determination: Ann Cavoukian, *Privacy in the clouds. A white paper on privacy and digital identity: Implications for the internet*, p. 7.

- Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (hereinafter referred to as: EU Data retention Directive 2006/24/EC)
- National Law

The key statements of these legal frameworks in respect to the basic principles of privacy and their consequences for the requirements of realising data protection will be determined and analysed in the following sections.

2.2 EU Data Protection Directive 95/46/EC

In a world more and more concerned with digital data processing, data protection and privacy are significant issues.[12] In this context, the EU Data Protection Directive 95/46/EC is the main document to look for as a legal foundation to deal with these issues within the European Union. This section will address the general scope of this Directive to give an overview in respect to the importance of this framework. It will then give insight to jurisdictional questions primarily in respect to the provisions of "personal data" and determination of involved parties. However, the further specific provisions to apply data protection law within the scope of the EU Data Protection Directive 95/46/EC will be discussed under section 3.1.6 "Determining the applicable law" as well as under section 3.3. "Critical factors for data protection in cloud computing" (there under subsection 3.3.2.1 "Jurisdiction") for specific cloud computing scenarios.

2.2.1 Scope of legislation

The protection of personal data is the main objective of the EU Data Protection Directive 95/46/EC. It also aims at harmonising the Data protection law of the European member states to achieve a more universal effectiveness of protection and also support the internal market through enabling a free flow of data. Since the first discussions about the data protection at the United Nations Conference on Human Rights in 1968, privacy and the protection of personal data has become increasingly significant. As a consequence of the growing awareness of privacy as a conditio sine qua non for personal freedom, the EU Data Protection Directive 95/46/EC finally came into legal force on 24 October 1995.

As a part of the European integration process, the Directive constitutes the protection of fundamental human rights and makes them one of its main objectives. So recital (1) of the EU Directive 95/46/EC refers explicitly to the Convention for the Protection of Human Rights and Fundamental Freedoms:

[12] Cf. Rafael Capurro, *Privacy – An Intercultural Perspective*, Ethics and Information Technology (2005) 7: 37-47, which contains a comparative examination of privacy in Europe an Japan; see also Ian Brown, Oxford Internet Institute, University of Oxford, *Working Paper No. 1: The challenges to European data protection laws and principles* of 20 January 2010 in the context of the European Commission's *Comparative Study on different approaches to new privacy challenges in particular in the light of Technological developments.*

(1) Whereas the objectives of the Community, as laid down in the Treaty, as amended by the Treaty on European Union, include creating an ever closer union among the peoples of Europe, fostering closer relations between the States belonging to the Community, ensuring economic and social progress by common action to eliminate the barriers which divide Europe, encouraging the constant improvement of the living conditions of its peoples, preserving and strengthening peace and liberty and promoting democracy on the basis of the fundamental rights recognized in the constitution and laws of the Member States and in the European Convention for the Protection of Human Rights and Fundamental Freedoms.

These objectives are the basis for the subject matter of the EU Data Protection Directive 95/46/EC in an all-embracing manner. The provisions and requirements of lawful data processing in the scope of this Directive always must be considered with these general objectives of fundamental human rights in mind.

2.2.2 Personal data as jurisdictional precondition

However, there is the question of jurisdiction under the EU Data Protection Directive 95/46/EC. The Directive explicitly states that it shall apply especially for the right to privacy.[13] It then refines this objective by establishing the respect for fundamental rights and freedoms of individuals always when the processing of personal takes place. So there are three main preconditions for the applicableness of the Directive. These are: data being concerned, data being processed and this data being personal. "Data" is generally abstract information which defines a single or several attributes in a set of variables. In this context, the Directive is worded in a technology-neutral way since it does not require the automated processing of data. Rather, according to Article 2 lit. b), any processing of personal data evokes the applicableness of the Directive.[14] According to Article 3 (1), non-automated means of processing are encompassed into to scope of the Directive if being wholly or partly part of any filing system. The different exemplary means of data processing mentioned in Article 2 lit. b) of the Directive is by no means an exhaustive list and makes it possible to subsume other data usage methods under the generic term of “processing”. This unbiased phrasing enables a protective effect without being per se detrimental to new technical developments and changes on the national and international markets. The technological changes in Europe encompass the increasing usage of computers, digital cameras, mobile phones, and other mobile equipment with the ability to interconnect to each other. More and more often, biometric and electronic identifiers are used to associate users to devices and subscribed services.[15] In the context of cloud computing, the processing of data is the typical case. Cloud computing is a more and more commonly proposed and used business model, whereas offered services to a large extent involve the processing of data. We assume that the EU Data Protection Directive 95/46/EC can apply to processing of data in all of these contexts due to the fact that it is focused on the act of data processing as such and not on the technology that is used for this act.

[13] See recitals (2) and (3) of the EU Data Protection Directive 95/46/EC.

[14] See Article 2 lit. b) EU Data Protection Directive 95/46/EC.

[15] The Article 29 Working Party concludes similarly on the so-called “data deluge” effect, see WP 173, *Opinion 3/2010 on the principle of accountability*, adopted on 13 July 2010 p. 4; The Article 29 Working Party was set up on account of Article 29 EU Data Protection Directive 95/46/EC, which demands the formation of a working group “on the Protection of Individuals with regard to the Processing of Personal Data”. It functions as an independent advisory group counselling the European Commission in respect to data protection and privacy issues.

The central jurisdictional requirement of the EU Data Protection Directive 95/46/EC beyond the processing of data is this data being personal. According to Article 2 lit a) of the Directive, any information relating to an identified or identifiable individual ('data subject') is considered a personal data. Due to this restriction to natural persons, governmental institutions, corporate bodies and other legal entities are not subjected to the protection of the EU Data Protection Directive. The Article 29 Data Protection Working Party presented an in-depth analysis of the concept of personal data whereas it clarified that information being related to an "identified" individual means doubtlessly distinguishing this individual among a group of several persons. "Identifiability" opens up the possibility to distinguish an individual that has not been identified yet. Since the latter is the lower level in regard to the identification of an individual, it is to be considered as the threshold condition in regard to this element of the personal data definition.[16] So identifiability in the sense of the Directive is given if the information conveys a connection to a particular physical person, no matter if this connection happens directly or indirectly, already took place or is still a mere possibility. Such information could be for example the name, address, telephone number, a civil registration number or an email address that could be linked to the data subject.[17] Also geolocation data is being considered as being personal.[18]

Even statistic data might be personal data if the target group is small enough to relate information to a specific person of this group. Also data which conveys information about race, ethnicity, political opinion, religion or philosophical beliefs, health or sex life of an individual is personal data which is considered having a high level of sensitivity.

We will now investigate the provision of personal data being concerned as a precondition to the applicableness of the EU Data Protection Directive 95/46/EC specifically in the context of cloud computing. Firstly, this preconditions the determination of what kind of data is typically processed in a cloud environment. Cloud Computing can convey the offer of the most diverse services in the IT field. The most basic service models as explained by the NIST, are Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service, providing fundamental IT resources, such as applications, storage, computing power, networks and development platforms.[19] These basic service models however, are quite insufficient to depict the whole range of products and services in the cloud computing field. IT vendors offer a multitude of service concepts with most diverse consequences for processing personal data in such a cloud environment.[20] Therefore, it is essential to take the individual

[16] Article 29 Working Party, WP 136, *Opinion 4/2007 on the concept of personal data*, adopted on 20th June 2007, p. 12.

[17] Similarly, the OECD Guidelines defines personal data as such, see Section B in the detailed comments, paragraph 41.

[18] See the statement of the Article 29 Working Party, WP 185, *Opinion 13/2011 on Geolocation services on smart mobile devices*, adopted 16 May 2011, p. 7.

[19] The National Institute of Standards and Technology (NIST) is a federal authority located in the United States of America, which focuses on measuring and developing science and technology standards. In January 2011, NIST published a cloud computing definition, which introduces the characteristics, service models and deployment ways in the cloud computing field. This definition was being reviewed and re-presented in the May 2011 special publication *Cloud Computing Synopsis and Recommendations*. For the definition of the three basic service models, see section 2-1.

[20] We are providing an exemplary role model with a more detailed description of possible products and services in Annex A of this document. Still, the NST definitions are a well recognised fundament to roughly categorise popular cloud services. Another good overview with tangible examples is presented by Chakraborty, Ramireddy, Raghu and Rao in their collaborate paper *The Information Assurance Practices of Cloud Computing Vendors*, p. 30, published by the IEEE Computer Society 2010.

services themselves and the factual circumstances into account instead of focusing on rigid categories. These individual services involve mostly sets and databases of anonymised, pseudonymised, encrypted and fragmented data in the cloud for purposes of storage and processing in any way. Consequently, the question arises if such data can also be considered as being personal as the relation of the data to the individual concerned person is at stake. In some cases, determining if specific types of data are personally identifiable information can prove exceedingly difficult. For instance, the legal status of IP-addresses as identifiers in respect to certain natural persons is subject to lively and intense discussions on technical level as well as from the legal point of view.[21] Also, the question if encrypted data can be classified as information relatable to certain persons has been the subject of many debates.[22] In this context, some opinions state that in this case the data should be considered as personal data in regard to the keyholder of the encrypted information only.[23] Other views state that the encryption does not cause any different designation as personal data, depending on the effectiveness of preventive measures against the reversibility of the data into plain text form.[24] Another case of doubt would be the fragmentation of data into parts, where the automated "sharding" for digital storage may arise the question of this data still being information relatable to an individual, hence personal data.[25] Whenever the data cannot be classified as being personal, it falls out of the protection scope of the Directive. However, national law still could apply since the EU member states are empowered to extend the scope of the Directive as long as no other regulation in the EU legal framework prevents it. However, the scope of the Directive should be interpreted with a broad view since the ultimate goal of the EU Data Protection Directive 95/46/EC is the protection of individuals and their personal data.

In the light of this objective, the intentions of the decision-makers on European level who developed this Directive in its legislative process must be kept in mind and taken into consideration whenever the application of the provision "personal data" is in question. So in cases of doubt, it may be more appropriate to assume personal data is involved.[26]

[21] See the following working documents of the Article 29 Working Party on this subject: WP 148, *Opinion 1/2008 on data protection issues related to search engines*, adopted on 4 April 2008 p. 8 and WP 136, *Opinion 4/2007 on the concept of personal data*, adopted on 20th June 2007, p. 16 f.; controversial views are represented in White, *IP Addresses Are Personal Data, E.U. Regulator Says*, The Washington Post published January 22, 2008.

[22] An assessment will be made for the context of cloud computing a later section of this report under 2.3.1. ("Jurisdiction").

[23] W. Kuan Hon, Christopher Millard, Ian Walden, Queen Mary University of London, School of Law Legal Studies Research Paper No. 75/2011, *The Problem of 'Personal Data' in Cloud Computing - What Information is Regulated? The Cloud of Unknowing, part 1*, p. 25 ff.

[24] Article 29 Working Party, WP 136, p. 18; also see Ross Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*, chapter 5 (2nd edition 2008) for a non-mathematical elucidation of one-way and two-way encryption .

[25] Ibid., Kuan Hon, Millard, Walden, footnote 20, p. 11.

[26] The Article 29 Working party represents the same view in its WP 136, see p. 4f. for a comprehensive reasoning.

2.2.3 Parties involved and responsibilities[27]

To safeguard the protection in respect to personal privacy, the EU Data Protection Directive 95/46/EC provides several types of involved parties to enable the allocation of legal accountability. According to Article 2 lit. d) and e) of the Directive, the roles of data controllers and data processors are of particular significance. Hence, the following two subsections will be the most in-depth in respect to these two roles and outline their differences in status and responsibilities. The third section will thus briefly present other roles encompassed through the Directive but with less significance in regard to the allocation of responsibilities.

2.2.3.1 Data controllers

According to Article 2 lit d) of the EU Data Protection Directive, a controller is a "natural or legal person, public authority, agency or any other body which alone or jointly with others determine the purposes and means of the processing of personal data". The wording of the Directive clarifies three main provisions for the determination of an entity as data controller. These three provisions are:

a) A natural or legal person, public authority, agency or any other body

b) determines the purposes and means of the processing of personal data

c) alone or jointly with others

These three provisions will be explained briefly in the following.

a) Natural or legal person, public authority, agency or any other body

The first provision highlights that not only natural persons may be considered being a controller but also e.g. companies, governmental bodies and other public authorities. So it is explicitly stated that the legal form of the active entity does not play a role in regard to the question if it could be a controller. Hence natural and legal persons are equated in terms of determination of their role and the corresponding responsibility.

b) Determination of purposes and means of the processing of personal data

As second provision, Article 2 lit d) emphasises that the controller is the one who determines the purposes and the means of the data processing. This emphasises the control over the "if, why and how" of the data processing. This decision power is the main factor to determine if someone is a controller. Together with Article 6 (1) and Article 23 of the EU Data Protection Directive 95/46/EC, this decision power establishes the liability of the controller for the compliance of the data processing with the legal obligations of the Directive. Only in cases when the controller is able to actively rebut his responsibility for any damaging event, he could be released of the liability. Therefore, the responsibility remains in principle with the controller. However, to specify if someone is the determining person or legal body, one must

[27] Due to linguistic and legal system diversity in the European countries, the term “responsibility” is often used with dissimilar meanings. Also, other words with corresponding or rivalling relevance are for example be “accountability”, ‘”reliability”, “obligation” and “reinforced responsibility”. In this document, we define and use the term „responsibility“ with focus rather on the consequences of non-compliance in terms of legal data protection requirements. In this context, also the term „accountability“ may be used. See also the WP29, Opinion 3/2010 on the principle of accountability, adopted on 13 July 2010 p. 7 f. for a comparable usage of these terms.

have a closer look at the de-facto situation in which the data processing takes place. Especially in cases, where several parties with unknown status are involved, the clear determination of controller and processor can be exceptional challenging. Therefore, the Article 29 Data Protection Working Party provides some criteria to ascertain if a party is in control of the processing, hence a data controller. These criteria are:

- Explicit legal competence
- Implicit competence
- Factual influence.[28]

The explicit legal competence means that the actor is designated by national or Community law to be the controller of a data processing. Such a direct assignment by the law is in principle the exception. Still some assignment could stem indirectly, if an entity is by law instructed to perform certain tasks for which the collection and processing of data by this entity is essential. So, for example, governmental bodies for which it is absolutely necessary to collect and process data to fulfil its public function, are to be considered as controllers.[29]

The implicit competence results from conventional roles conveyed through common legal provisions or established legal practice, such as civil law, commercial law, labor law, etc. These are roles with functional or organisational power, mostly held by legal bodies. In this context, the Article 29 Data Protection Working Party cites the employer and the publisher as controllers in regard to data of employees or subscribers.[30]

The most profound criterion is that of the factual influence on the data processing. In regard to purpose and means of the processing, this means that it is important to carve out who is the person or legal body who autonomously initiated the data processing in the first place and defined the purpose of it. Secondly, it is of importance, who specifically stipulated what shall happen with the data.[31] This influence is the most principal factor to appoint an entity as controller and in the following determine its responsibilities.

All these three criteria help to define if the actor can be considered being a data controller. Additional factors to support this assessment will be presented later in the following section 2.1.2.3.2 (Data processors). The responsibilities resulting of the determination of an entity as controller are generally regulated through the EU Data Protection Directive. These are fleshed out as obligations of the controller on the one hand and as tangible rights of the data subject on the other hand.

The obligations of the controller, according to the text of the Directive, are:

- Information of the data subject about
  - the identity of the controller and his representative, if any
  - the processing purpose
  - recipients/categories of recipients of data
  - if a response to the questions is obligatory or voluntary, the means to response and consequences of failure to reply
  - the data subject's right to access and rectify the data concerning him.

[28] Article 29 Working Party, WP 169, *Opinion 1/2010 on the concepts of "controller" and "processor"*, adopted on 16 February 2010, p. 10 ff.

[29] Ibidem.

[30] Ibid.

[31] Ibid., p 11.

  - further points to guarantee a fair processing, if necessary.[32]

- Additionally, in cases of data obtainment through third parties
  - the categories of data concerned, except in cases the data is processed for statistical purposes or historical or scientific research or in cases of impossibility, disproportionate effort of legal prohibition.[33]
- Provision of appropriate technical and organizational measures to safeguard the security of processing.[34]
- Notification of the appropriate supervisory authority with information about the data processing.[35]
- In cases of doubt about the lawfulness of the processing, consult the appropriate supervisory authority for prior checks

These obligations determine a liability of the controller in cases of data processing, which is not compliant with the provisions of the data protection law. However, they are not concluding regulations of the lawfulness of data processing. Rather, they complement the data subject's rights, which are also codified by the EU Data Protection Directive.

These rights are:

- Giving consent, unless the data processing is already legally permitted.[36]
- Access to the data concerning him, incl. eventual rectification, erasure or blocking.[37]
- To object the processing of the data concerning him.[38]

The precise preconditions and means of realising these rights of the data subject will be discussed in section 2.3.1.1 (Realisation requirements - Information, choice and consent). However, these regulations on obligations and rights may differ or be limited under certain provisions, such as the processing solely for purposes of journalism, literary or artistic expression or other processing's that imply a reconciliation of the right to privacy with the freedom of expression.[39] Nevertheless, they are the basic framework conditions under which lawful actions of the controller can take place.

c) Action alone or jointly with others

The third provision of Article 2 lit. d) EU Data Protection Directive 95/46/EC is that not only a single entity could be a controller, but also together with others. Hence, the shared responsibility of several entities may be possible. The decisive factor here is the joint control that the several entities have over the processing of the data. Indicators of such could be contractual arrangements as well as shared de-facto control over the handling of the data. However, this preconditions that the acting entities are separate bodies and not linked in a

[32] See Article 10 EU Data Protection Directive 95/46/EC.

[33] See Article 11 (1) lit. c) EU Data Protection Directive 95/46/EC.

[34] See Article 17 (1) EU Data Protection Directive 95/46/EC.

[35] See Article 18 and 19 EU Data Protection Directive 95/46/EC.

[36] Cf. Articles 7 lit. a) and 8 (2) lit. a) EU Data Protection Directive .

[37] See Article 12 of the Directive.

[38] See Article 14 of the Directive.

[39] See Article 9 of the Directive.

way that they could be seen as one entity. This may be relevant for companies and their subsidiaries, where it sometimes can prove difficult to determine if they are really separate legal structures. According to the legal assessment of the Article 29 Data Protection Working Party, the joint control should mirror the single control be determined with a substantive and functional approach as well.

Decisive factors or criteria could be:

- Contractual agreements of the actors involved
- Factual circumstances, such as executive power[40]

However, an equal distribution of the decisive power, regardless of being on contractual or factual basis, is not necessary. Due to the most diverse constellations possible once several actors are involved, it can't be relevant if all controllers have the same degree of control over the whole data processing. Instead, the remaining amount competence in the sphere of each controller must be of relevance. Cases of shared infrastructure, sequenced processing, combined processing activities can cause the designation of joint control as well as the so-called "origin-based approach", where each data controller is responsible for the data being processed in his own system. Still, in complex cases, it may prove difficult to determine if there is any distribution and shared exercise of control over the data processing. Therefore, the construct of joint control should be understood as means to eliminating uncertainties by assuming the existence of several controllers instead of a controller-processor constellation. This interpretation with a broader scope for responsibility allocation makes it easier to ensure data protection compliance in favour of the data subject.[41]

Finally, it can be said, once all these aforementioned requirements of Article 2 lit. d) EU Data Protection Directive 95/46/EC are fulfilled, an entity involved can be considered as data controller. In the following section, we will make a comparative contemplation of the role of the data processor to enable a more detailed carving out of the specific characteristics of data controllers and processors.

2.2.3.2 Data processors

Counterpart of the data controller is the data processor. According to Article 2 lit. e) EU Data Protection Directive 95/46/EC, the processor is "a natural or legal person, public authority, agency or any other body which processes data on behalf of the controller". This wording highlights two main provisions for a classification of an actor as processor of data:

a) Different identity than the controller

b) Processing of data on behalf of the controller

These two legal preconditions will now be outlined in the following.

[40] Article 29 Working Party, WP 169, p. 18.

[41] Ibid., pp. 18 ff.

a) Different identity than the controller

What is obvious as a simple condition laid down in a legal framework may not be as easy in complex situations. We have to turn to the specific real life case and have a look if the actors involved can be considered as different entities or not. This can be solved mostly in terms of legal disparity. An example would be the actions of a company's employee within the boundaries of his or her duties. If the company is a data controller, the employee is not a processor acting on behalf of the company because from a legal point of view, his or her actions are regularly attributed to the employer. So it can be said that an actor acting under direct legal authority, e.g. as staff person, cannot be a data processor. In contrast, whenever an actor represents a completely separate legal entity, he can be distinguished from the role of the controller.[42]

b) Processing of data on behalf of the controller

So once a separate controller entity is identified, it is crucial to determine if the actor in question processes data on behalf of this controller. This means that he undertakes data processing tasks that were delegated to him from the controller. The pivotal factor is the processor's decision power over the purpose and means of the processing. The processor must be prevalent bound by the instructions of the controller. This leads to a limited liability of the processor only within the boundary of his duties towards the controller. So, the responsibility (respective accountability) for any data collection, processing and storage is closely connected to the classification of involved parties as either data controllers or data processors. The specific criteria of explicit legal competence, implicit competence and factual influence to differentiate between controllers and processors were already presented in the prior section. Nevertheless, the Article 29 Data Protection Working Party compiled additional criteria that can support the identification of an actor as processor of data. These additional criteria are:

- Level of prior (contractual) instructions
- Monitoring through the controller entity
- The visibility or outward appearance of the data controller towards the data subject
- Professional expertise as service taking precedence over the data processing
- Margin of manoeuvre left to the processing party due to new means of processing
- Level of knowledge and decision power on controller side[43]

These criteria can help ascertain the role of the processing entity. This determination is important for the differentiation between processor and controller entity, which again is crucial for the allocation of responsibility for the compliance in respect to the EU Data Protection Directive 95/46/EC. This allocation enables the application of the Directive and makes it possible to enforce the necessary compliance with the data protection law in the further.

[42] The Article 29 Working party represents the same viewpoint in its WP 169, p. 25.

[43] For an in-depth elaboration on these criteria with example cases, see footnote above, p. 24 ff.

2.2.3.3 Other roles

Article 2 lit. f) and g) of the EU Data Protection Directive 95/46/EC constitutes two additional roles that may be relevant in respect to data processing. These are the roles of the "third party" and of the "recipient". A third party is "any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or processor, are authorized to process the data". Hence, it is an entity which is an outsider without any contractual or legal authorisation to access and process personal data of someone else. Regardless of lawful of unlawful obtainment, this entity can be, once it receives personal data from somewhere, also be a new controller under the provisions of the EU Data Protection Directive. This includes all aspects of legal obligations and responsibilities as well.[44]

According to Article 2 lit. g) sentence 1 EU Data Protection Directive 95/46/EC, a recipient is "a natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not". However, sentence 2 of Article 2 lit. g) excludes authorities who receive data in the framework of a particular inquiry. So, according to the text of the Directive, the determining factor for this designation is the act of data being disclosed to this entity. Hence "recipient" is to be understood as a mere denomination based on an action of an involved party.

We have now presented these different roles and highlighted their importance for the allocation of responsibility in regard to the processing of personal data. The determination of an entity being a controller, processor, third party or recipient is crucial for any legal obligation getting assigned to an involved party to enable an all-embracing protection of the data subject's rights without leaving loopholes. Hence, it is essential to always have a close look at the circumstances of the individual cases and the activities of these involved parties. We will take such a closer look in terms of cloud computing cases later in this document under section 2.3. "Critical factors for data protection in cloud computing" (there under subsection 2.3.4 "Involved parties, responsibilities and lack of enforcement"), where we will identify the difficulties arising in this context.

2.3 E-Privacy Directive and related/amending Directives

As another basis for the protection of personal data and privacy of individuals, the so-called E-Privacy Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector inclusive its amending Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 has to be taken into account. Also, we will briefly amplify the related Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and the Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, which were both also amended by the 2009/136/EC Directive. We will present these frameworks and their application scope in terms of data protection in the following.

The E-Privacy Directive 2002/58/EC addresses in Article 1 (1) its subject-matter to the effect, that this Directive shall be applicable in the field of electronic communication networks and services to end-users. It shall enable the availability of "good-quality publicly available services through effective competition and choice and to deal with circumstances in which the needs of end-users are not satisfactorily met by the market".[45] Within this scope, "this

[44] Ibid. p. 31

[45] Article 1 (1) Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (E-Privacy Directive) in its amended form within Article 1 Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009.

Directive defines the minimum set of services of specified quality to which all end-users have access, at an affordable price in the light of specific national condition without distorting competition".[46]

Unfortunately, neither this Directive nor the amending Directive present a definition of the terms "electronic communication networks and services" and "end-user". Instead, the E-Privacy Directive 2002/58/EC refers in its Article 1 to the definitions laid down in Article 2 of the Framework Directive 2002/21/EC.[47] These define the aforementioned terms as follows:

- Article 2 a) Electronic communications network

  "Electronic communications network" means transmission systems and, where applicable, switching or routing equipment and other resources which permit the conveyance of signals by wire, by radio, by optical or by other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched, including Internet) and mobile terrestrial networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable television networks, irrespective of the type of information conveyed."

- Article 2 c) Electronic communications service

  "Electronic communications service" means a service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting, but exclude services providing, or exercising editorial control over, content transmitted using electronic communications networks and services; it does not include information society services, as defined in Article 1 of Directive 98/34/EC, which do not consist wholly or mainly in the conveyance of signals on electronic communication networks."

- Article 2 h) & n) End-user

  "User" means a legal entity or natural person using or requesting a publicly available electronic communications service". "End-user" means a user not providing public communications networks or publicly available electronic communications services."

One of the main elements of these definitions is the public availability of such networks and services. In this, the scope of the Directive has a quite broad scope. Still, the related Framework Directive 2002/21/EC clarifies that the e-Privacy Directive is not focused on content of services delivered over electronic communication networks using electronic communications services.[48]

These definitions set the scope for the E-Privacy Directive to the effect that in respect to cloud computing, we have to investigate whether cloud services cover the electronic communications sector as outlined in these definitions. It may be that some of them convey the provision of electronic communication via services or networks according to the above definitions. Hence, the point is to discover if the individual cloud service is provided to make the electronic communication in the sense of the Directive possible. Cloud computing can convey a multitude of most different services, such as application provision as well as computing power, storage or hardware services. In this context, the most likely use case may be the enabling of electronic communication networks as defined in Article 2 a) Framework Directive 2002/21/EC. Hardware services provided may enable the transmission of signals in

[46] Ibid., Article 1 (2) Directive 2002/58/EC, amended by Article 1 Directive 2009/136/EC.

[47] Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive).

[48] See recital (5) of the Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive).

the first place to make such electronic communications possible. Also, an improvement of signal conveyance via the provision of computing power is thinkable. In respect to electronic communications services, as defined in Article 2 c) Framework Directive 2002/21/EC, such services that focus on the remuneration may be provided via cloud computing too.

Furthermore, according to the definitions of Article 1 (1) of the E-Privacy Directive 2002/58/EC, these services must be publicly available. This is a precondition that is only partly applicable to cloud computing services. Some of the offered services in the cloud computing field may only be provided to a single costumer, as it would be in the case of an implemented private cloud infrastructure. Also, the services offered to a community cloud could not be considered as being publicly available, since in this case the group of service users is known and limited. A subsumtion under this precondition of the Directive may only be possible for public cloud services which are available to everyone. In these cases, the applicableness of the Directive is given in cases of public cloud services which fall under the scope of the aforementioned Framework Directive 2002/21/EC definitions.

2.4 EU Data Retention Directive

On European level, also Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks (hereinafter referred to as Data Retention Directive 2006/24/EC) must be considered as relevant in regard to the legal data protection framework. This EU Data Retention Directive 2006/24/EC, which partially amends the E-Privacy Directive 2002/58/EC, was adopted as a legislative regulation to enable measures to combat terroristic activities. It is thereby a political reaction to the terroristic attacks of in New York 2001 and Madrid in 2004. This Directive was and still is discussed most controversial due to its restrictive nature in regard to the right to private life and correspondence as laid down in Article 8 of the European Convention on Human Rights and fundamental Freedoms (ECHR).[49] In this context, it is subject to significant criticism related to its necessity and effectiveness. This concerns the data retention period as well as the number of data to be stored and the data protection and security measures. It is also still not accurately implemented in all EU member countries due to constitutional concerns.[50]

The scope of the Directive is laid down in its Article 1, which states that it is focused on the regulation of data retention to enable the access of law enforcement authorities for a certain period if necessary as a means for prevention, investigation and prosecution of serious crime as defined by each of the member states in its national law. To achieve this, the scope of the Directive is aimed at a harmonised regulation of the obligation of providers in the publicly

[49] For instance, see the European Data Protection Supervisor Peter Hustinx, *Opinion on the Communication from the Commission to the European Parliament and the Council - "The EU Counter-Terrorism Policy: main achievements and future challenges"* of 24 November 2010 and the ruling of the Czech Constitutional Court of March 31st 2011 on the national implementation of the Directive in the Czech Republic. This ruling followed prior decisions of the constitutional courts in Germany and Romania.

[50] European Data Protection Supervisor Peter Hustinx, *Opinion on the Evaluation report from the Commission to the Council and the European Parliament on the Data Retention Directive (Directive 2006/24/EC)* of 31 May 2011; see also Article 29 Working Party, WP 172, *Report 01/2010 on the second joint enforcement action: Compliance at national level of Telecom Providers and ISPs with the obligations required from national traffic data retention legislation on the legal basis of Articles 6 and 9 of the e-Privacy Directive 2002/58/EC and the Data Retention Directive 2006/24/EC amending the e-Privacy Directive*, adopted on 13 July 2010, p. 8 ff.

available electronic communications services or public communications networks sector. In this context, it applies the definitions of the EU Data Protection Directive 95/46/EC as well as the definitions laid down in the E-Privacy Directive 2002/58/EC and Directive 2002/21/EC.[51] Moreover, it clarifies the scope in regard to the term "data" in its Article 2 (2) lit. a), whereas it is made clear that the Data Retention Directive 2006/24/EC applies solely to traffic data and location data and the data necessary to identify the subscriber or user. These data are further specified in Article 5, which in detail entails which categories of data shall be retained. This encompasses such data as telephone numbers, names, addresses, user ID's date, time and duration of a communication, type of communication, International Mobile Equipment Identity, digital subscriber line and geolocation data. The scope of the Directive however, does not entail the content of the communication.[52] Thus, in regard to cloud computing, the applicableness of this Directive must be assumed since the business model of cloud computing is strongly based on the access to services via networks. This would most likely encompass such data relating to electronic communications services or public communications networks.[53]

The execution of the data retainment is specified in the Directive Article 6, which determines the possible periods of retention from minimal six months to maximal two years. The E-Privacy Directive stipulates a restriction of its scope in a way that member states are authorised to decree legislative measures in regard to "national security, defence, public security and the prevention, investigation, detection, and prosecution of criminal offenses or of unauthorised use of the electronics communications system, as referred to in Article 13 (1) of Directive 95/46/EC".

Further, it explicitly refers to the implementation of a data retention regulation as such a measure.[54] This retainment, however, stands in conflict with the general principles of data minimisation and purpose-binding as laid down in the EU Data Protection Directive 95/46/EC and the E-Privacy Directive 2002/58/EC. Data protection issues are tackled in the context of the Data Retention Directive just in such a way that for the retainment of the data, certain data protection and security safeguards must be ensured through appropriate technical ands organisational measures. These safeguards must be pursuant to the provisions of the EU Data Protection Directive 95/46/EC and the E-Privacy Directive 2002/58/EC. However, these safeguards are not specified enough yet. Concluding, we come to the result that the EU Data Retention Directive is applicable to certain data types, respectively traffic data, location data and the data needed to identify the concerned user or subscriber. Therefore it must be considered for the offer and usage of cloud services to determine which obligations the providers of such services will have to fulfil.

[51] Article 2 (1) Data Retention Directive 2006/24/EC.

[52] Ibid., Article 5 of the Directive.

[53] Ibid. footnote 52, in which it was acknowledged that the Data Retention Directive may apply to cases of outsourcing due to the fact that it may be related to several activities in regard to traffic data.

[54] Article 15 (1) Directive 2002/58/EC.

2.5 National Law

Finally, going downward from the supranational level, national law must also to be considered as a basis for the regulation of data protection and privacy. The principle of direct application of national law contemplated already in the Treaty on the functioning of the European Union, which states in its consolidated version in Article 288 (ex Article 249 TEC) that

> *"A directive shall be binding, as to the result to be achieved, upon each Member State to which it is addressed, but shall leave to the national authorities the choice of form and methods."*

So the EU member states are empowered to regulate the matters laid down in EU Directives different as they see fit for their own needs. This is often specified in the individual Directives on European level, such as in Article 13 EU Data Protection Directive 95/46/EC, where the EU member states are allowed to make specific regulations for example in matters of state security, inner security, defence and the prevention, investigation and prosecution of criminal offenses.

According to Article 5 of the EU Data Protection Directive 95/46/EC, the EU member states are explicitly allowed to adopt the Directive into their national law pursuant to its conditions. For instance, such conditions are laid down in several Articles of the Directive, in particular Articles 4, 17 and 28. This also implies that in certain areas, the EU member states are authorised to extend their individual national law beyond the scope of EU Data Protection Directive 95/46/EC. For instance, Article 5 EU Data Protection Directive 95/46/EC demands the further determination of the conditions for lawful data processing by the member states. So the rough requirements laid down in the Directive can be shaped into more detail by the EU member states. In this, these states are given the freedom to add tighter restrictions for lawful data processing than they are provisioned in the EU Data Protection Directive. For instance, in Germany, the national data protection law has an additional ten point's catalogue for cases of a processor processing data on behalf of a controller, demanding the contractual and factual implementation of certain preconditions. This ten point's catalogue encompasses the realisation of data subject's rights and also obligations of the service provider, which he needs to fulfil to make any data processing by a processor lawful.[55] The Italian data protection law authorises the local data protection authority to give out binding deontology and codes of conduct for specific sectors that must be met by civil and public law entities.[56]

Another example would be the processing of certain categories of data, which is regulated in Article 8 of the EU Data Protection Directive 95/46/EC. The processing of sensitive data, such as health data, may be only lawful under certain preconditions, which in some cases, the EU member states can further specify individually. So in Italy, the national data protection law (Codice in materia di protezione dei dati) provisions that if the data of a minor shall get processed, e.g. for needed medical treatment, the consent of the parents shall be obtained. Moreover, once the minor becomes and adult, another explicit consent by this concerned data subject is mandatory. [57] Hence, in such cases the consent is given twice since the first consent given by the parent do not have a continuing legal effect. The Italian government thus implemented the recommendations made by the Article 29 Working Party concerning

[55] See Article 11 BDSG (Bundesdatenschutzgesetz) of Germany.

[56] Article 12 (1) di Codice in materia di protezione dei dati (personali Decreto legislativo 30 giugno 2003, n. 196).

[57] Ibid., Article 82 (4).

the protection of children's personal data, whereas in other EU member countries, the general consent rules of the EU Directive has not been specified in that way.[58]

Further example for the lack of harmonisation in regard to the implementation of the EU legal framework derives from the EU Data Retention Directive, which enables the EU member states to regulate the retention period individually and gives only a rough provision of a retention period from six months to two years. This leads to quite different implementations of this Directive in each of the member states, conveying retention periods that may vary greatly. If an EU member country does not implement the requirements of the EU Data Protection Directive 95/46/EC into its national law within the determined time frame, the provisions of the Directive come into effect directly. So to this date, the harmonised implementation and interpretation of the EU Data Protection Directive 95/46/EC and its related Directives into the national law of the EU/EEA countries is still deficient.[59]

Additionally, in cases of cross-border offered services, there is also the necessity to be compliant with the specific legal requirements of each individual state in which this service is available. In the context of the TClouds project, it is not possible the regard the data protection law of each EU member state which may be relevant for the project use cases. With respect to the scope of the project, such an in-depth legal analysis will therefore not be provided. Instead, we will focus on the European level with the EU Data Protection Directive 95/46/EC as the superior framework and just involve national law as far as it will be relevant for the project-internal use cases. This will involve mostly the use-case-relevant Portuguese law from the energy sector and Italian law from the health sector. The analysis of the specific national requirements will be provided in the upcoming reports R1.2.2.1 (Specific legal analysis and requirements: "Smart Lighting") and R1.2.2.2 (Specific legal analysis and requirements: "Patient Monitoring"). Moreover, in the following section, we will investigate the means to determine the applicable law in regard to data protection and privacy.

2.6 Determining the applicable law

The EU Data Protection Directive 95/46/EC is the main framework which roughly defines the protection goals and general measures in respect to the personal freedom of individuals, especially in regard to privacy. As already described in the prior section, the EU Data Protection Directive 95/46/EC does not come into direct legal force in the EU member countries. Instead, these countries are obliged to transfer these general guidelines into their national law and thus specify the detailed means of the Directive's objectives. The EU Data Protection Directive 95/46/EC however, outline the rough provisions under which the applicable law can be determined.

[58] See Article 29 Working Party, WP 147, *Working Document 1/2008 on the protection of children's personal data (General guidelines and the special case of schools)*, adopted on 18 February 2008.

[59] See *First report on the implementation of the Data Protection Directive (95/46/EC)* of the Commission of the European Communities, Brussels, 15.5.2003.

(http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2003:0265:FIN:EN:PDF) and the thereto relevant study sponsored by the European Commission on *Different approaches to new privacy challenges, in particular in the light of technological developments*, 20 January 2010, (http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_en.pdf).

The EU Data Protection Directive 95/46/EC distinguishes between three possibilities to determine which national law may be applicable in cases of personal data processing. These three possibilities are:

- The activities of an establishment of the controller in one of the EU member countries, (Article 4 (1) lit. a) of the Directive)
- Applicableness of national law by virtue of international public law,

  (Article 4 (1) lit. b) of the Directive)
- Usage of automated or non-automated equipment for data processing, located in an EU member country, except for purposes of mere data transit,

  (Article 4 (1) lit. c) of the Directive)

These possibilities are conclusive. The Directive does not provide explicitly for any other legal grounds for the applicableness of EU law, e.g. by contractual means. Of the three possibilities, the most crucial provision for the applicableness of the European Data Protection Directive 95/46/EC is the location of the establishment of the controller entity. Unfortunately, the Directive does not provide a further definition of the term “establishment”. Nevertheless, in the context of the Directive’s purpose to protect data subjects and regulating the legal liability and obligations of the controller, recital 19 of the Directive states that “establishment on the territory of a Member State implies the effective and real exercise of activity through stable arrangements; whereas the legal form of such an establishment […] is not the determining factor in this respect”. So the scope of the Directive is directed at the focal point of the controller’s activities for the data processing act itself. The importance establishment as business concept in general derives from Article 50 of the Treaty on the functioning of the European Union (ex Article 43 TEC), which emphasises the freedom of establishment as a particularly valuable contribution to development of production and trade. The European Court of Justice clarified in one of its rulings[60], that the establishment must entail the permanent presence of the human as well as the technical resources, which are necessary for the provision of the offered services. In also clarified in another ruling, that the term ”establishment” must refer to a sufficient physical presence, either by staff or any kind of other business structure in which agreements or management decisions may be taken.[61] The Article 29 Data Protection Working Party interpreted this ruling as refusal to acknowledge computer means as a virtual establishment and therefore drew the conclusion that in most cases, a server or computer is not to be considered as an establishment in the sense of the Directive. Rather, it must be considered as a mere technical facility or instrument for the data processing. [62]

Also, an office that only fulfils representative functions rather than being a location where decisive activities take place is not being considered as an establishment. Crucial criteria for the determination of the establishment are the degree of involvement of the establishment(s) in the concrete processing activities and the nature of the activities themselves. In this context, these precise activities of processing personal data are also decisive to determine who the controller is in the first place. Therefore, this first step is closely connected to question of the controller’s establishment. Furthermore, the applicableness national law may be triggered in several EU member states in cases of the controller having more than one

[60] European Court of Justice (Second Chamber), decision of 4 July 1985 in the case Gunter Berkholz v Finanzamt Hamburg-Mitte-Altstadt, p. 2265 (C-168/84).

[61] European Court of Justice (Fifth Chamber), decision of 7 May 1998 in the case Lease Plan Luxembourg SA v Belgium (C-390/96).

[62] Article 29 Working Party, WP 179, *Opinion 8/2010 on applicable law*, adopted on 16 December 2010, p.11 f., with elaboration on exemplary use cases.

establishment, which is also considered possible. However, it is sufficient to have at least one establishment in one of the EU member countries to apply the Community law. As a general rule, this may be company headquarter or principal office of the vendor. The statutory seat of the controller, where the purpose and means of the data processing are determined, must be considered as an establishment in the sense of the Directive. Still, other establishments, which are separate from the company's headquarters, are possible.[63] Whenever a controller has no establishment at all which is located within the territory of the Community, it may also possible that the Community law is applicable through international public law.[64] These are generally the cases of applicableness of EU law in an embassy or consulate, on a ship or airplane, as long as these locations are in some way governed by international agreements or a special jurisdictional status by international law.[65]

The third possibility of EU data protection law applicableness would be the usage of equipment for the processing of personal data. In this context, it does not matter if this equipment is automated or not. It solely depends on the question if this equipment is located in an EU member country and not used for purposes of mere data transit only. If this EU-located equipment is used for the data processing, then EU law may apply even if the controller has his establishment outside the Community territory.[66] It also may apply if the controller has an establishment within the EU but this establishment is not in any way relevant for the data processing in question.[67] The Article 29 Data Protection Working Party interpreted the term "equipment" in a broad sense of the word, considering the fact that in other languages versions of the EU Data Protection Directive other than English, the relevant article uses a term rather to be translated as "means" of data processing. Following this broad interpretation, we assume than human as well as technical intermediaries can be "equipment" in some way as long as these are not solely used for the transfer of the data through the EU territory but also for processing of the data within the Community area. Also, outsourcing activities executed by data processors can be considered as being equipment used by the controller. [68]

The determination of applicable law demands a closely inspection of the individual cases of personal data processing that takes all of the above criteria into account. We will investigate these specific criteria and their impact to situations arising in a cloud computing context in the later Sections 3.3 ("Critical factors for data protection in cloud computing"), 3.4. ("Challenge: Cross-border disclosure of personal data") and 3.5. ("Cloud Computing: Methods of resolution"). Due to the nature of the EU Data Protection Directive 95/46/EC as main superordinate framework, the scope of this deliverable will focus on the details of the legal requirements on this EU level. Further analysis related to the TClouds use cases and the specific national law which may be relevant, will be provided in the later reports R1.2.2.1 (Specific legal analysis and requirements: "Smart Lighting") and R1.2.2.2 (Specific legal analysis and requirements: "Patient Monitoring").

[63] Ibid., p. 12 f., with a comprehensive listing of example cases.

[64] Article 4 (1) lit. b) EU Data Protection Directive 95/46/EC.

[65] Article 29 Working Party, *Opinion 8/2010 on applicable law*, p.18.

[66] Article 4 (1) lit. c) EU Data Protection Directive 95/46/EC.

[67] Article 29 Working Party, WP 179, p. 19.

[68] Ibid., p. 20.

Chapter 3

Realisation requirements

This chapter briefly introduces the specific requirements of the EU Data Protection Directive 95/46/EC as the most significant legal construct for data protection within the European Union, respective the European Economic Area. These requirements convey five main criteria to guarantee an effective protection of personal data in the sense of the Directive. These five criteria are:

- Information, choice and consent
- Predetermination for specific purposes
- Data minimisation
- Security safeguards
- Compliance, accountability and enforcement

We will present these criteria and their legal foundation within the EU Data Protection Directive and highlight their impact on the protection of personal data in the following subsections.

3.1 Information, choice and consent

The processing of personal data that falls under the scope of the EU Data Protection Directive must fulfil certain criteria to be legitimate. So amidst other legitimisations, the most significant criterion is the explicit consent by the concerned person, namely the data subject.[69] However, it is necessary that some conditions can be recognised to the effect that the given consent is valid. So in its Article 6 (1) a), the Directive generally demands that data should be processed fairly and lawfully. This means that the data subject must be able to have all knowledge and decision power for being able to exercise his own rights. Consequently in the sense of this transparency requirement, this means that the concerned individual must have the factual possibility to learn that his data is being processed. Furthermore, he must have accurate and full information on the circumstances of the collection of his data. This encompasses the information about the data disclosure to a third party as well as data breach notifications.[70] The requirement of data breach notifications as such is not regulated explicitly in the EU Data Protection Directive 95/46/EC. The E-Privacy Directive however, delegates by its Article 4 (5) powers to the European Commission to adopt technical implementing measures concerning the circumstances, format and procedures applicable to the information and notification requirements. Hence, services that fall into the scope of the E-Privacy Directive also trigger the applicableness of data breach notifications under this Directive.

[69] Article 7 a) EU Data Protection Directive 95/46/EC.

[70] See recitals (38) and (39) of the European Data Protection Directive 95/46/EC as well as Article 4 (5) E-Privacy Directive

3.2 Predetermination for specific purposes

The processing of personal data must be predetermined for a specific purpose. This provision of a certain purpose is another ground of making the processing legitimate and is restricted legal basis, contractual necessity or another, essential interest of the data subject explicitly regulated in the EU Data Protection Directive or by national law. The further processing of the data is generally prohibited as long as it is incompatible with the original purpose that initiated the collection of the data in the first place. [71] So for such processing, further legitimising grounds are also necessary or else wise the data shall be effectively deleted.

3.3 Data minimisation

Recital (28) of the EU Data Protection Directive 95/46/EC demands that the collection of the data for purpose-specific processing shall not be excessive. This is a provision that in a reverse conclusion, not more data than it is absolutely necessary for the processing in the individual case shall be collected.

3.4 Confidentiality and security safeguards

According to Articles 16 and 17 of the EU Data Protection Directive 95/46/EC, specific confidentiality and security safeguards must be provided for to ensure the protection of the data. Such safeguards can be the binding to the instruction of the controller, the prevention of unwanted disclosure (limited disclosure to processors, subcontractors and third parties only on legitimate grounds) and the prevention of undesired data destruction, loss, corruption or deletion and other unlawful forms of processing. Furthermore, the controller must ensure that these confidentiality and security safeguards also come into effect once a processor processes the data on his behalf. In this context, the Directive explicitly refers to appropriate technical and organisational measures that shall be taken to realise these safeguards.[72] Recital (46) of the Directive clarifies that such measures shall be taken both at the time of the design of the processing system and during the processing itself. It also demands a sufficient balancing of the state of the art in terms of possible security level, implementation costs and the risks of the processing act. Which technical and organisational security measures as mentioned in Article 17 (1) are appropriate highly depends on nature, manner and purpose of the data processing, the facilities and the organisational structure of the data controller. Thereby, a distinction is made between logical and physical security measures.

Examples for logical security measures relevant in the context of cloud computing are:

- encryption of data
- data separation
- transmission security
- use of secure communication channels
- access to data is logically restricted

[71] For instance, see Article 6 (1) lit. b) for the general requirement of purpose-binding and Article 8 EU Data Protection Directive 95/46/EC for the processing of special categories of personal data with the authorisation of the EU member states to regulate specific purpose cases; also, see recitals (28), (30) and (31) of the Directive.

[72] Article 17 (1) European Data Protection Directive 95/46/EC

- strong authentication; and the use of (biometric) tokens
- risk assessment
- security certification/audit
- penetration tests
- intrusion detection systems
- access log management
- logging of system admin
- log files audit trail
- appointed Chief Information Security Officer (CISO)
- appointed Computer Emergency Response Team
- standard for data handover to subcontractors or corporate branches

Examples for physical security measures are:

- written policies (and penalties for breaches)
- storing of backups in a different place than the server itself
- limited access rights
- physical access control
- systems against intruders
- alarm response centres
- security guards
- video surveillance
- fire detection systems/ fire extinguishing systems
- water/flood protection
- overvoltage protection
- emergency power supply/redundant power supply

Regarding the TClouds use cases, several specific requirements for technical and organisational measures ensue to effectively secure the individual sector-specific data (health data and smart lighting data). Especially for the home health care scenario, enhanced security measures for the health care and hospital sector will have to be taken into account to ensure the appropriate protection of sensitive health data. When making personal data anonymous is considered a priority, e.g. for scientific research purposes, matters of design also involve how to organise data processes and products. A typical instance is given by the processing of patient names in hospitals via information systems: Here, patient "names and other personal identifiers maintained in hospitals' information systems should be separated from data on the health status and medical treatments. They should be combined only in so far as it is necessary for medical or other reasonable purposes in a secure environment".[73] Likewise, in accordance with the principle of controllability and confidentiality of the data to be processed, biometric and other highly sensitive identifiers should be stored in devices

[73] Article 29 Working Party, WP 168, The Future of Privacy, p. 14.

under control of the data subjects (i.e. physical activity monitoring device) rather than in external data bases. [74]

3.5 Compliance, accountability and enforcement

The realisation of an effective protection of personal data requires the compliance of the processing act with the provisions of the EU Data Protection Directive and the relevant national law, the accountability of the responsible parties, namely the controllers and the enforcement of this legal responsibility. These requirements are supported by several provisions laid down in the Directive. For instance, such provisions would be the notification of supervisory authorities and prior checking, publicising of processing operations (Articles 18-21) as well as judicial remedies, liabilities and sanctions (Articles 22-24) and the sphere of activity, respective scope of authority of the aforementioned supervisory authorities. According to the individual regulations of the EU Directive, these provisions need to be shaped into detail and implemented by the EU member states into their national law. Hence, for each processing of personal data, the question which national law is applicable is vital for the efficiency of the data protection in the individual cases.

[74] Article 29 Working Party, WP 168, The Future of Privacy, p. 14.

Chapter 4

Critical factors for data protection in cloud computing

This section will investigate the legal hurdles that arise in the interplay between the cloud computing field and the European data protection framework. Focusing on the principles and provisions of the EU Data Protection Directive 95/46/EC, we will highlight legal uncertainties that tackle issues of jurisdiction, factual control over and third-party-access to personal data. We will also examine questions of individual case-assessment in respect to identifying the actors, their legal responsibilities and difficulties of data protection enforcement.

4.1 Jurisdiction

As we elucidated in Section 2.1.2.2 (Personal data as jurisdictional precondition) above, a crucial provision for the applicableness of the EU Data Protection Directive 95/46/EC is the processing of personal data. Vital for the success of the business model of cloud computing is the security of the data, e.g. via encryption. There are, however, some uncertainties if the handling of encrypted data is a case of processing personal data in the sense of the EU Data Protection Directive. Personal data are data that relate to an identified or identifiable individual. For this determinability, the knowledge, means and possibilities of the processing entity is most relevant. But what if the processing entity does not have the decryption key but only the data subject himself?

If encrypted data shall be stored in some database, the cloud system would have to ensure that all data transmissions between the provider and the customer are secure and already encrypted. The encryption of data and processes e.g. in the sphere of a cloud storage service provider would have to be realised like a fully encrypted hard disk of which only the customer has the key. To exclude the possibility of data tapping between data- and transmission encryption or the extraction of the key out of the RAM, the system need to have some "tamper resistance". This shall enable the customer to learn and verify any unauthorised access to the data. Effective methods already exist in the cloud computing field but are still not distributed widely. More complex is the encryption of data in a virtualised environment. Methods of “boxing” (e.g. placement of virtualisation into an encrypted environment through a corresponding hypervisor) and fully homomorphic encryption can be approaches to be developed further to guarantee more security in this field.

The point is, however, that every seemingly uncrackable encryption technique will be decryptable within few years with simple, even automated methods. So under the provisions of knowledge, means and possibilities of the processing entity, it is not sufficient to focus on the present state of the art only. This would be detrimental to the purpose of the EU Data Protection Directive since the uncertainty, if and when the decryption of the data can be realised with realistic and doable methods, can not be allowed to the expense of the data subject in need of protection of his personal data. Moreover, the “security” of an encryption technique is not per se provable. Security metrics for such techniques will always retain

some not estimate-able uncertainty.[75] So the assumption that data in encrypted state is not personal cannot be made on the basis of not provable encryption effectiveness. Furthermore, the encryption of data is essential precisely because the data is personal. Therefore, the encryption can only be seen as a technical measure to protect the data in the sense of Article 17 (1) EU Data Protection Directive. If we see the provision of personal reference for the application of the Directive as absolute value, the data must always be considered as personal as long as someone has the key.

Another provision for the applicableness of the Directive is the establishment of the controller. As we already discussed in Section 2.1.6 ("Determining the applicable law"), the determination of this establishment can prove difficult in some cases. Consequently, we will have to look at the factual circumstances in terms of controller activities in an individual case assessment. [76] Such factual circumstances must relate closely to the personal data that is being processed within the offered cloud service. In a first step, the controller of the service agreement needs to be identified. This can prove challenging especially in a cloud computing context, where either provider or customer of a service (or both) could be located outside the EU or several providers or customers could be involved. The statutory seats of cloud service providers could generally be identified as establishments in the sense of the Directive since these are locations from where the providers pursue the management of their business. Also, the statutory seat of the cloud service customer is an establishment, since from there the customer dictates the purpose and means of the data processing. This location is therefore the centre of his activity.

In some cases, the focal point of activities can not be as easily identified in the context of cloud computing since the nature of such services is the remote offering of services. Thus it may be possible, that the focus of activities does not lie at the location of the service provider or the customer, but concentrates on server facilities of the provider or even in the virtual machines (hereinafter: VMs)[77] used to process data. Due to the ruling of the European Court of Justice, mere computer means or virtual presence of the controller are not sufficient to acknowledge an establishment of the controller.[78] So, especially in regard to VMs, the establishment of a controller cannot be assumed. Instead, they must be seen solely as an instrument for the processing operations.[79] This view is especially significant in respect to the fact that virtual machines always have a physical machine as host but can also be transferred or deleted easily. Also, the location of such virtual machines on a physical host may not be predetermined but follows distribution in reaction to the workloads of the physical machines. Therefore, it seems more reasonable to take the location of these physical hosts, namely the server farms and data bases, into consideration primarily.[80] These server farms and data centres can be considered as being an establishment of the controller as long as they serve the purpose of being a focal point of the controller's activities. During the EU-funded OPTIMIS project, four core elements were identified to ascertain if such a server facility can be classified as an establishment. These are economic activity, factual pursuit of

[75] Cf. Marten van Dijk, Ari Juels, *On the Impossibility of Cryptography Alone for Privacy-Preserving Cloud Computing*, published 2010, which gives a good overview over the weaknesses of cryptography techniques as exclusive measure to safeguard privacy in a cloud environment.

[76] Article 29 Working Party, WP 179, p. 12.

[77] Virtual machines in an cloud computing environment are isolated operation systems that either execute software or virtualises hardware functions just like a physical machine.

[78] European Court of Justice (Fifth Chamber), decision of 7 May 1998 in the case Lease Plan Luxembourg SA v Belgium (C-390/96).

[79] Cf. Article 29 Working Party, WP 179, p.11 f.

[80] The legal assessment of Barnitzke et al. for the EU-funded Optimised Infrastructure Services (OPTIMIS) project comes to the same conclusion in its Deliverable D7.2.1.1 – Cloud Legal guidelines, p. 38 f.

this activity, fixed establishment or stable arrangement and an indefinite period for this location being such a focal point of activity. These elements highlight that in some cases, server centres often can be considered as establishments in the sense of the Directive. This applies also to partially remote hardware care and administration by human staff, since the performance of the server centre is affected directly.[81]

Nevertheless, it must be investigated if the provision of equipment, as laid down in Article 4 (1) c) EU Data Protection Directive, can also be applicable due to the remote provision of cloud services via networks. So an assessment, if a server facility can be considered as equipment in the sense of the Directive is needed. The broad scope of the term "equipment" allows an understanding of this provision as "means" of processing the personal data. The question is, if such a broad interpretation of this term is desirable since it leads to a very widespread application of the EU Data Protection Directive. As we already discussed above, these means of processing can consist of human as well as solely technical facilitators.[82] Data centres with their physical machines are mostly technical means to realise the processing of the personal data. Human intermediaries can be the administrators of the server farms, who directly influence their operating performance. So both human and technical measures are used as means of processing. In this context, difficulties arise mostly from the fact that not even the cloud service providers do not exactly know which data are processed in which data centre. In such cases, it may be more reasonable to primarily take the statutory seats of provider and customer for the criterion of establishment into account. Even this may prove insufficient for the applicableness of the EU Data Protection Directive 95/46/EC if no connection to EU territory can be made at all. This may lead to a gap of applicableness if the controller's establishment and also his equipment are located outside the EU/EEA whilst the concerned data subject is living within the Community area. Hence, the broad scope of the term "equipment" is favourable against the risk of leaving a protection gap at the expense of the data subject.[83]

Thus, data centres and server farms can be considered as "equipment" in the sense of the directive as long as they are significantly relevant to the processing act in question. Consequently, the knowledge of their location should be a prerequisite if data protection under EU law is desired.

4.2 Outsourced control

One of the most significant problems of cloud computing is the loss of the customer's direct influence on security and privacy measures to protect his data. Moreover, the remote processing of data and often standardised contractual binding to predefined privacy and security settings of the provider impede and hinder the immediate control not only of the service customer but also of the data subject himself. Many cloud service providers, especially those with global market power, pursue a strategy of little transparency to protect their own business concepts. Therefore, supervisory authorities may take the view that the processing of personal data in a cloud environment may under certain circumstances not be compliant with the legal requirements of the EU Data Protection Directive 95/46/EC.

[81] Ibid., p. 39 f. with reference to the case law of the European Court of Justice and recital 37 of the Directive 2006/123/EC of the European Parliament and the Council of 12 December 2006 on services in the international market.

[82] Cf. Article 29 Working Party, WP 179, p. 20 on outsourcing activities.

[83] Ibid. p. 31 f.

So the Datatilsynet Danish Data Protection Agency issued an opinion regarding the cloud service of Google Apps for a Danish municipality, stating that the processing of confidential and sensitive data require some specific security and data protection safeguards. Such safeguards are:

- An explicit legal basis for the data processing
- An adequate risk assessment, conducted by the municipality as controller
- A contractual agreement that ensures the compliance of the processor entity with the controller's instructions
- Factual feasibility of compliance control, namely in respect of knowledge of data centre locations
- Technical and organisational measures, such as adequate deletion of data, secure transmission and login, rejection of unauthorised attempts to access data and means of logging[84]

In its opinion, the Danish Data Protection Agency took the view that transparency is a mandatory precondition to enable the service customer to realise the compliance of the data processing act in respect to the legal protection requirements. So the customer must ensure not only that the service vendor provides tangible contractual commitment but also gives him the factual possibility to verify the compliance. If the customer does not have this kind of reassurance, the lawfulness of the data processing is questionable at best. Thus, the customer may not be permitted to use such cloud services. In this context, customers often perform inadequate risk assessments in regard to the specific cloud computing context.[85]

Also an issue of lack of transparency and control are breach notifications. These are a vital element of damage limitation and control for the customer and ignite the basis of trust so the (potential) customers of the cloud know how their data are secured and protected. While the E-Privacy Directive laid the legal grounds for such data breach notification, they are not yet mandatory in most EU member countries. There are however, correlated legislation processes in the making that strive to find a comprehensive regulation for this issue. Still critical is the question when a data breach should be assumed. According to a related ENISA report about this topic published in January 2011, some criteria to consider a breach could be:

- Loss of IT equipment – misplaced or stolen equipment – laptops, USB sticks, etc.
- Mailing – distribution of a letter in the mail or an email to an incorrect address that includes personal data
- Improper disposal of documents – leaving personal data in documents deposited in a garbage bin that can be accessed by the public
- Hacking – malicious attacks on computer networks
- Technical error – unforeseen complication in an IT system exposing data to outside parties
- Theft – data in the form of documents, electronically stored data, etc. that is stolen

[84] See the Opinion of Datatilsynet, the Danish Data Protection Agency Copenhagen K: *Regarding processing of confidential and sensitive personal data in connection with use of Google Apps online office suit* of 3 February 2011, p. 3.

[85] This was also a point of criticism in the Opinion of the Danish DPA, see p. 6 f., where it stated that a general risk assessment based on the SAS 70 Type II Certification is not sufficient for the specific cloud-related context of the case.

- Unauthorised access – employees taking advantage of vulnerabilities to access personal data of customers stored in files or electronically
- Unauthorised distribution – distributing personal data on P2P networks

Also, it was pointed out, that the type of the data (like sensitive data, e.g. health data) is important qualitative indicators for more detailed criteria and an even broader approach to the assumption of data breaches.[86] Also, the definition of risk and tangible notification and handling procedures are a central discussion subject.[87]

Another critical problem in terms of control may be the business consistency. Vendor-lock-in is an issue as well as the bankruptcy of service providers. Especially in cases of big data bases, the migration of them from one vendor to another data is still intricate if not impossible.

Consequently, these facts about loss of direct control on customer and data subject side lead to unacceptable factual and legal uncertainties. As long as these are not resolved, they will significantly hinder the business model cloud computing to evolve on a wider market.[88]

4.3 Access of third parties

The processing of personal data in a cloud computing system on remote virtual and physical machines entails increased risks of third party access to that data. There may be three different types of access that may happen upon data that are given into the sphere of a cloud service provider. These are:

- Access of outsider attackers
- Access of insider attackers
- Access of investigation bodies

In the following, we will give an overview of these parties' possibilities to access data that is stored and processed in the cloud and analyse the impact on the requirement of data confidentiality and security.

4.3.1 Outsider attackers

A third party involvement in regard to personal data is the unauthorised access of an outsider attacker. This is not an entity which is either customer or provider of the cloud service, or any other entity directly related to the data processing in question. Outsider attackers may use a variety of different attack methods, e.g. such as distributed denial of service (DDoS, causing the unavailability of the service), password cracking, spoofing, viruses, worms and key loggers. Their actions may be differently driven, e.g. by challenge, protest or profit

[86] European Network and Information Security Agency (ENISA), *Data breach notifications in the EU*, published January 13, 2011, p. 16 f.

[87] Ibidem, p. 18 f.

[88] Cf. Neil Robinson, Lorenzo Valeri, Jonathan Cave & Tony Starkey (RAND Europe) Hans Graux (time.lex) Sadie Creese & Paul Hopkins (University of Warwick), *The Cloud: Understanding the Security, Privacy and Trust Challenges* - Final Report for Directorate-General Information Society and Media, European Commission, 30 November 2010, p. 35 ff. on the growing focus on security and privacy in cloud computing.

motivations. This kind of illegal access is the most classical issue in terms of computer security in general and not exclusively reserved for the cloud computing field. Nevertheless, the outsourced control over the data regularly forces the customer of the service to rely solely on the security policies of his provider. Hence, it becomes impossible for the customer to accomplish his own adequate security requirements despite increased risks for the security of the personal data.

4.3.2 Insider attackers

Another kind of third party access is the case of insiders. An "insider" is typically someone who has generally legitimate access to the cloud service system. Such a person could be an employee of customer or cloud service provider, a contractor, business partner or anybody else who has generally authorisation to access the cloud service. Such access however, must be differed from the access to the data processed through this service. Generally, in terms of computer security and data protection, we can differ between non-malicious (such as the honest-but-curious) insider and the malicious insider, depending on the motivation of the actor involved.[89] On customer side, it is imaginable that the employee of a company which uses the cloud service, accesses data for other, non-operational purposes (such as industrial espionage) or even despite not having explicit access authority for this kind of data (e.g. because of being a worker for a different functional area in the company). On provider side, it may be possible that the provider, respectively employees of the provider, access data that they are not authorised for to pursue other purposes than the processing of data on behalf of the customer. Other constellations are also possible. So on customer side as well as on provider side, the misuse or unintentional corruption of data is an issue that is often underestimated. [90]

Another issue is the increasing use of automated systems for indecency checks for censoring intentions.[91] The European E-Commerce Directive, regulating provider liability privileges foremost in the field of hosting, caching and conduit services, lacks clarity, effectiveness and harmonisation. So the foggy legal situation in respect of provider liability for harmful and illegal content may cause an overly extensive removal of data on uncertain legal grounds.[92] Even more complexities arise once the provider involves several sub-contractors to process the personal data. For the users of cloud services the risk of malicious insiders is, however, the most severe threat that still does not get adequate attention despite some root approaches to this topic. The reason for this is the uncertain legal situation as well as the factual power of the provider of the cloud service.[93] Therefore it is a considerable issue in the cloud computing field.

---

[89] Anton Chuvakin, *Insider Attacks: The Doom of Information Security Methods to thwart insider attacks: products, techniques and policies*, 2002, p. 2 f.

[90] Cf. Uhl/Kern, *Datenmissbrauch am Arbeitsplatz – eine Herausforderung für Personalmanager*, German study published on 22/03/2011 by CMS Hasche Sigle in cooperation with Kroll Ontrack.

[91] For an example, see Microsoft's PhotoDNA, a program designed to undeceive child pornography on public servers, which scans images on disproportional percentage of skin display (http://www.microsoft.com/presspass/presskits/photodna/) Such automated processes precondition access to personal data of the customer that the data subject generally is not aware of.

[92] Hotly debated is the notice-and-takedown procedure without court order. Similarly, this problem is also an issue in non-European context, cf. the corresponding regulations of the US Digital Millennium Copyright Act (DCMA).

[93] One approach is the IaaS-focused research of Francisco Rocha and Miguel Correia, see their paper *Lucy in the Sky without Diamonds: Stealing Confidential Data in the Cloud.*

4.3.3 Investigation bodies and supervisory authorities

Due to the transmission of data into a cloud environment, the legitimate access of investigation bodies and supervisory authorities also is an issue. Article 13 EU Data Protection Directive 95/46/EC authorises EU member states to restrict some of the regulations of the Directive for areas of national security, defence, public security, crime prevention, investigation, detection and prosecution. Also, a restriction may be possible in areas of monetary, budgetary and taxation matters as well as in regulated matters of monitoring, inspection or regulation functions of certain bodies and the protection of the data subject himself or the rights and freedoms of others. Also, according to 28 (3) EU Data Protection Directive 95/46/EC, supervisory authorities shall be equipped with investigative powers, effective powers of intervention and powers to engage in legal proceedings to fulfil their duties. More legislative power results from the Council of Europe Convention on Cybercrime (hereinafter referred to as CoECC). This convention was drafted with the intention of encountering new types of crime emerging with the increasing use of information technologies around the world. Also the commitment of traditional crimes by means of new technologies shall be covered by the convention. It takes into account the fact that crimes being committed via information technologies potentially can be more far-reaching in their consequences because geographical restrictions and legal boundaries to national territories become less effective.[94] The CoECC conveys territorial jurisdiction[95] as well as thematic jurisdiction for cloud computing cases. In regard to aforementioned thematic relation, Chapter II Section 1 Title 1 (Offenses against the confidentiality, integrity and availability of computer data and systems) and Chapter II Section 1 Title 2 (Computer related offenses) are the most relevant in terms of cloud computing.[96] Also relatable to the cloud computing context is the Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters. Another example would be the disclosure of personal data that is processed by service providers established in the United States due to the U.S. Patriot Act and other legal grounds.[97] In conclusion: what all of these frameworks have in common, is that they convey the member states' legislative power to regulate the legitimate, governmental seizure of personal data that is located within the cloud system.

[94] Council of Europe, Explanatory Report to the Convention on Cybercrime, section I. (ETS No. 185).

[95] Article 22 of the CoECC.

[96] See Articles 2-6 and 7-8 of the CoECC; for a comprehensive analysis of the applicableness of the Cybercrime Convention see Cristos Velasco San Martin, Director General of the North American Consumer Project on Electronic Commerce (NACPEC), *"Jurisdictional aspects of Cloud Computing"* pp. 5 ff.

[97] So the U.S. based company Microsoft admitted in a publication at ZDNet on June 28, 2011 that European personal data based in a cloud may be exposed to U.S. investigation bodies by the Patriot Act; publication is to be found at: http://www.zdnet.com/blog/igeneration/microsoft-admits-patriot-act-can-access-eu-based-cloud-data/11225. Microsoft also published additional information for its customers in its Online Services Trust Center, (http://www.microsoft.com/online/legal/v2/?docid=23), where it is stated that Microsoft U.S. companies and also their EU-based subsidiaries may disclose personal data to any governmental law enforcement body. Under the provision of a National Security Order (NSL), this disclosure may even happen under a gag-order, so in this case Microsoft will not notify the customer of the service.

4.4 Involved parties, responsibility and lack of enforcement

The perhaps most critical issue from legal point of view in terms of cloud computing is the question who is legally responsible for the processing of personal data. According to the EU Data Protection Directive 95/46/EC, the controller entity is the responsible party. The identification of the controller, however may prove challenging. The main problem in cloud computing context is the increasing layering of services and vendors. This is due to the more and more common combination of ancillary services from different providers by the customers as well as unified main services and communications, which are offered by the vendors.[98] Also the contractual allocation of responsibility is a prominent characteristic of the market power of some internationally operating cloud service providers. The ToS and Privacy policies of such providers (e.g. Amazon, Google, and Microsoft) are standard forms, in which the conditions of data protection and security are mostly unilateral arrangements, for which the right of change is universally reserved. This stands in direct conflict with the EU Data Protection Directive and the related national data protection law requirement that the processor (provider) of personal data may only act on instructions by the controller (customer/subscriber). Also, this factual control of the provider over the processing hinders the customer to actively and directly supervise the compliance of the data processing with the legal data protection requirements. But this significant loss of control is detrimental to the generally remaining legal responsibility on the side of the customer as controller of the data processing. Therefore, the clarity of any contractual allocation of obligations and rights in relation to the provider of the service is crucial to decrease key business and compliance risk factors.[99]

Furthermore, the enforcement of such compliance is a critical matter. The interpretations and opinions of the Article 29 Data Protection Working Party are not legally binding advice towards the EU Commission and the EU member states. Rather, they are recommendations that are well acknowledged within European data protection authorities. These supervisory authorities also have limited possibilities to enforce the data protection compliance. The authorisations regulated in Articles 22-24 (Remedies, Liability, Sanctions) are vague and open to the interpretation by the EU member states. Therefore, the implementation of investigative and sanction powers of the data protection authorities considerably lacks harmonisation within the community area.[100] Moreover, collective civil redress is not compatible with the legal systems of some EU member states due to the assumption, that civil procedure law can only serve the individual enforcement of subjective rights solely. So, the European Commission plans to introduce a harmonised European contract law. But so far, the civil enforcement is insufficient in cases of cross-border data processing.[101]

Another open question is the performance of compliance auditing in respect to the European data protection requirements. Logging measures must ensure the comprehensibility of processes for standard checks by supervisory authorities as well as in cases of data

[98] W. Kuan Hon, Christopher Millard, Ian Walden, Queen Mary University of London, School of Law Legal Studies Research Paper No. 75/2011, *The Problem of 'Personal Data' in Cloud Computing - What Information is Regulated? The Cloud of Unknowing, part 1*, p. 7.

[99] Cf. Siani Pearson, Andrew Charlesworth, *Accountability as a Way Forward for Privacy Protection on the Cloud*, 6 August 2009, proposing an approach on technical and procedural solutions for this issue.

[100] European Union Agency for Fundamental Rights, *Data Protection in the European Union: the role of National Data Protection Authorities - Strengthening the fundamental rights architecture in the EU II*, 2 February 2011, p. 19 ff.

[101] European Union Agency for Fundamental Rights, *Access to justice in Europe: an overview of challenges and opportunities*, 23 March 2011, p. 36.

Centrum für Europäische Politik (CEP), Communication COM(2010) 245 of 19 May 2010*: A Digital Agenda for Europe*, p. 4.

breach/corruption incidents. The Datatilsynet Danish Data Protection Agency demanded that logs shall at least provide information about time, user, type of use and an indication of the person the utilised data referred to, or the search criteria used. In its opinion in the Odense Municipality/Google Apps case, it criticised that Google did not provide such substantial information about how these logging requirements are met.[102]

Also the regulation on breach notifications is still inadequate. Article 4 (5) of the E-Privacy Directive delegates powers to the EU Commission to adopt technical implementing measures in respect to such notifications. The transposition the E-Privacy Directive was due 25 May 2011. However, most of the EU member states have not yet adopted explicit data breach legislation.[103] Currently, in the context of the EU Data Protection Directive review, the European Commission is in the legislative process of an extension to complement the data breach framework of the E-Privacy Directive.[104]

[102] Datatilsynet, the Danish Data Protection Agency Copenhagen K: *Regarding processing of confidential and sensitive personal data in connection with use of Google Apps online office suit* of 3 February 2011, p. 14.

[103] Article 29 Working Party, WP 184, *Working Document 01/2011 on the current EU personal data breach framework and recommendations for future policy developments*, adopted on 5 April 2011, p. 6.

[104] European Commission, *A comprehensive approach on personal data protection in the European Union*, p. 4.

Chapter 5

Challenge: Cross-border disclosure of personal data

More complexities arise in cases personal data is being processed across borders, e.g. when the controller has his establishment in another country than the processor. In such cases, it is of importance if the parties are all located inside the European Union, respectively the European Economic Area or not. As we already elaborated above under section 2.1.6 (Determining the applicable law), the establishment of the controller is the main determining factor for the applicable national law under the umbrella framework of the EU Data Protection Directive 95/46/EC.

5.1 Third countries

If personal data is being disclosed across the borders of the Community area, the country in question must be referred to as “third country” in the sense of the EU Data Protection Directive. In such cases, the data processing on behalf of the controller according to the EU Data Protection Directive is only possible as long as the third country ensures an adequate level of protection.[105] If a third country does not provide such an adequate level of protection, the transmission of personal data is not per se permitted. So far, this adequate level of protection is acknowledged by the European Commission for the following countries: Andorra, Argentina, Canada, Faroe Islands, Guernsey, Isle of Man, Israel, Jersey, Switzerland and Uruguay. The transmission of personal data into a third country, which has not such an acknowledged level of protection, is generally prohibited according to Article 25 (4) of the EU Data Protection Directive. Additional safeguards are needed to make the data processing legitimate, for instance by the standard contract clauses provided by the European Commission (EU SCC). Also much discussed is the suitability of Binding Corporate Rules (BCR) and Codes of Conduct (CoC) to provide the needed level of protection for personal data. We will examine these tools in the later section 2.5 “Cloud Computing: Methods of resolution” (there under subsection 2.5.2 “Contractual and other regulations”).

5.2 The Safe Harbor exception

A special case is the United States of America, for which the European Commission has not acknowledged an adequate level of protection in the sense of the EU Data Protection Directive. Nevertheless, the transmission of personal data to U.S. located providers is supposed to be possible as long as the company is US Safe Harbor certified and complies with the corresponding requirements.[106] However, after over ten years of EU/US Safe Harbor

[105] See Article 25 (1) European Data Protection Directive 95/46/EC .

[106] Cf. Datatilsynet, the Danish Data Protection Agency Copenhagen K: *Regarding processing of confidential and sensitive personal data in connection with use of Google Apps online office suit* of 3

agreement, several studies have shown the factual problems of enforcement in this field.[107] So at this time, many European data protection authorities demand a close inspection of the certification and compliance with the agreement by the customer of the service.[108] A more in-depth analysis of the legal and factual issues concerning the Safe Harbor agreement will be provided in the following subsections.

5.2.1 Scope of Safe Harbor

The Safe Harbor Agreement came into being as a result of the necessity to balance and arrange the contending privacy and data protection frameworks of the EU and the USA. The European model of a comprehensive regulation has its counterpart in US system trusting in self-regulation and market forces.

Since the late 1970s there was the concern that data protection laws might be circumvented by transferring personal data to countries with lower or no standard regarding the protection of personal data, so called “data havens”[109]. Similar to the flow of capital to countries with low taxation and high profit expectations, a race to the bottom in data handling was impended.

Therefore, most data protection laws restrict the data transfer to third countries unless there are certain guarantees regarding the protection in the recipient country.

In the Council of Europe's 1981 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Article 12 restricts transborder flows of personal data. Article 25 of the European Data Protection Directive 95/46/EC imposes an obligation on member States to ensure that any personal information relating to European citizens is protected by law when it is exported to and processed in, countries outside Europe. It states:

> *"The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if the third country in question ensures an adequate level of protection."*

This requirement of adequate protection resulted in growing pressure outside Europe for the passage of strong data protection laws. Those countries that refuse to adopt meaningful privacy laws may find themselves unable to conduct certain types of information flows with Europe, particularly if they involve sensitive data. Determination of a third country's system for protecting privacy is made by the European Commission. The overarching principle in this determination process is that the level of protection in the receiving country must be "adequate" rather than "equivalent." Therefore, a reasonably high standard of protection is expected from the third party, although the precise dictates of the Directive need not be followed.[110]

February 2011, p. 4 ff., delving further into the issues of US companies with data centres located in the US and other third countries, when even the provider does not exactly know in which centre the data is actually located.

[107] See for example the Galexia Study by Connolly, *The US Safe Harbor – Fact or Fiction?*, 2008.

[108] See the resolution of the German supreme supervisory authorities for data protection in the non-public sector (Duesseldorfer Kreis) about Safe Harbor - PDF file in English: http://www.datenschutz-berlin.de/attachments/710/Resolution_DuesseldorfCircle_28_04_2010EN.pdf?1285316129.

[109] Michael, James (November 9, 1978). "New Report on Computer Data Banks", New Scientist, p. 432, http://books.google.com/books?id=tTs5-WSNM6AC&lpg=PA432&hl=de&pg=PA432#v=onepage&q&f=false.

[110] https://www.privacyinternational.org/article/overview-privacy.

The adequate level of protection required Article 25 of the EU Data Protection Directive 95/45 EC means that in addition to the general obligations of the data controller also the rights of the data subjects have to be safeguarded. When judging whether a non-European country provides this adequate level of protection all relevant circumstances for the data transfer and processing have to be considered. This concerns especially the requirements of Article 25 of the data protection directive with regard to the data subject's rights. Only few countries provide such legislation which is appropriate to the standards of the EU data protection framework

The United States of America have, from the European point of view, insufficient legal provisions in regard to privacy and data protection. For this reason, the transfer of personal data to the United States is inconsistent with the EU directive.

Complete severance of the data transfers between the EU and the USA, however, would have meant a considerable obstacle to international trade relations. To enable and promote the commercial relationship between the European Union and the United States, the EU-US Safe Harbor agreement was made by the US Department of Commerce and the European Commission in 2000. This agreement allows US companies to self-certify adherence to the Safe Harbor principles set by the US Federal Trade Commission (FTC). By submission to the principles the involved US companies should be regarded as providing an adequate level of protection within the company.

Legal basis for the recognition of this self-certification is the decision of the EC Commission of 26th of July 2000. The Commission recognises that US entities which publicly sign up to the agreement offer appropriate protection to personal data. As a result, data transfers to such organisations are considered lawful.

5.2.2 Historical development and origins

While all democratic states consider information privacy as a fundamental element of civil society, their approaches to ensure this element are quite distinct.

5.2.2.1 European Side

European governments emphasise information privacy as a critical element of social society. "[They] approach information privacy from the perspective of social protection. In European democracies, public liberty derives from the community of individuals and law is the fundamental basis to pursue norms of social and citizen protection. This vision of governance generally regards the state as the necessary player to frame the social community in which individuals develop and information practices must serve individual identity. Citizen autonomy, in this view, effectively depends on a backdrop of legal rights. Law, thus, enshrines prophylactic protection through comprehensive rights and responsibilities."[111] Due to their history of fascism and persecution, European states consider privacy as a fundamental human right, which does not only protect the individual's freedom against the private sector but also against interference of the state itself.

Therefore, European governments approached information privacy by means of public law. During the 1970s, the first European governments began to establish comprehensive information privacy and data protection regulations. These legislations all include in some way a guarantee of the individual's right to information self-determination. This premise of self-determination puts the individual in control of the collection and use of her personal data.

[111] Reidenberg, *testimony for the Hearing on the EU Data Protection Directive*, March 8 2001.

Consequentially, the laws also defined the responsibilities of data processors regarding collection, use, procession and disclosure of this personal data.

Regulation by establishing comprehensive data protection statutes was also on EU level the preferred way of dealing with information privacy. Although several appointed commissions considered the possibility of a system of self-regulation of the concerned authorities and companies as well, the vast majority opted for comprehensive data protection directive. Simitis, one of the main actors in the early stage of European privacy discussions, put in words the European scepticism towards self-regulation: "[It] seems rather doubtful whether such platitudinous propositions are of any help. […] Selfregulation […] proves […] to be at best an auxiliary measure."[112]

After a long process of negotiations the European Data Protection Directive 95/46/EC was adopted. Rather than conceding priority to business interests, European legislation sought to provide a high level of protection for citizens.[113]

This comprehensive and restrictive approach of the European Union inevitable invoked a substantial imbalance for transborder data flows. Compared to the European member states most other states provided an insufficient level of information privacy and data protection and were therefore feared to become data havens for personal data of European citizens. "Without the statutory authority to restrict transborder data flows, the balance of citizens' rights in Europe could easily be compromised by the circumvention of Europe for processing activities."[114]

In reply, the directive presented a provision to safeguard that personal data of European citizens will be treated according to European standards. Article 25 prohibits transborder data flows of personal data to countries that do not provide 'adequate' privacy protection.

This also included some of the major business partners of the European Union like the USA. To address the risk that the European member states would restrict the data transfer to the USA, the Department of Commerce started negotiations with the European Commission to establish a 'safe harbor' agreement.

5.2.2.2 US side

In opposition to the comprehensive European approach, the USA left the protection of privacy to markets rather than law.

Its privacy regime fits neatly into the liberal understanding of the government authority that the USA propagates. Unlike Europe, with its tradition of an active state authority holding the responsibility for regulating social relations, the USA emphasizes the ideal of a more restraint and restricted state authority, with more reticence towards economic momentum.[115] "[The] U.S. Congress has passed no overarching privacy law; explanations for this have ranged from First Amendment concerns and the free flow of information to the promotion of commerce and wealth, to a healthy distrust for governmental solutions."[116]

---

[112] Simitis *Establishing International Structures to Monitor and Enforce Data Protection*, 87f.

[113] Reidenberg, *testimony for the Hearing on the EU Data Protection Directive*, March 8 2001.

[114] Reidenberg, *testimony for the Hearing on the EU Data Protection Directive*, March 8, 2001.

[115] Fink, *Datenschutz zwischen Staat und Markt. Die „Safe Harbor"-Lösung als Ergebnis einer strategischen Interaktion zwischen der EU, den USA und der IT-Industrie*, 2002, 43f.; Hess, *American social and political Thought: a concise Introduction*, 2000: 37ff.

[116] Assey/Eleftheriou, *The EU-U.S. Privacy Safe Harbor: Smooth Sailing or Troubled Waters?*, 2001, 150; see also: Schriver, *You Cheated, You Lied: The Safe Harbor Agreement and its Enforcement by the Federal Trade Commission*, 2002, 2779

Consequently, the US Privacy Act of 1974 (5 U.S.C. § 552a, Public Law No. 93-579) only regulated the handling of personal data in the public sector. It did not establish an independent data protection authority but entrusted the monitoring of the Privacy Act to the Office of Management and Budget (OMB), a Cabinet-level office within the Executive Office of the President of the United States.

Section 5 of the Privacy Act established the Privacy Protection Study Commission (PPSC) to evaluate the statute and to issue a report containing recommendations for its improvement. The PPSC was a temporary commission created as a compromise to those who wanted a permanent data protection authority monitoring the impact of the Privacy Act. The Commission undertook several extensive hearings of US authorities and companies regarding their data handling standards.[117] Then in 1977, the PPSC issued its final report "Personal Privacy in an Information Society"[118] and ceased operation. The Report concluded that the 1974 Privacy Act "had not resulted in the general benefits to the public that either its legislative history or the prevailing opinion as to its accomplishments would lead one to expect".[119] In the report, the PPSC stated that, as transactions involving personal data have gained currency, there has been no compensating tendency to give the individual control over the collection, use, and disclosure of personal information.[120] The Report recommended that the President and Congress create an independent entity to participate in all federal proceedings affecting information privacy, including the issuance of guidelines that must be followed by federal authorities in interpreting the Privacy Act. However, the PPSC's recommendations were never passed by Congress nor addressed in any of the OMB's privacy guidelines.

Nevertheless, in contrast to its recommendations concerning the public sector, regarding the private sector the PPSC recommended a system of self-regulation as the method of choice.[121]

Though there are some laws stipulating the handling of personal data in specific areas of the private sector, these regulations "are often the result of a particular perceived crisis or 'horror story'"[122] and therefore only patch up exceptional cases, e.g. customer data of video libraries.[123] Therefore, the US privacy regulation of the private sector is sectoral and uneven.

5.2.2.3 Safe Harbor negotiations

Though at first in the US only few paid attention to European Data Protection Directive and its impact on international data flows, due to US privacy experts as Joel Reidenberg the danger of Europe shutting off its data transfers to the US proved impossible to ignore.[124]

With a trade value of $120.000.000.000 in transfer of personal data between Europe and the USA[125] at stake, the Clinton administration recognized the risk and began a "high-level, informal dialogue"[126] with the European Union in 1997.

---

[117] Personal Privacy in an Information Society, http://epic.org/privacy/ppsc1977report/ July 1977, 621ff.

[118] See Personal Privacy in an Information Society, http://epic.org/privacy/ppsc1977report/ July 1977.

[119] Personal Privacy in an Information Society, http://epic.org/privacy/ppsc1977report/ , July 1977, 502.

[120] Personal Privacy in an Information Society, http://epic.org/privacy/ppsc1977report/ July 1977, Epilogue 619 f.

[121] Fink 2002, 43.

[122] Reidenberg/Schwartz, *Data Protection Law and On-Line Services*:, 1998: 10.

[123] Video Privacy Protection Act 1988 (Pub.L. 100-618).

[124] Clear, *Falling into the Gap: The European Union's Data Protection Act and Its Impact on U.S. Law and Commerce*, 2000, 989.

Even before the official negotiations had begun, the White House emphasised in its Framework for Global Electronic Commerce the importance of the lead of the private sector.[127] The essential guidelines of the document underline that from the US point of view "[g]overnments should avoid undue restrictions on electronic commerce" and "[where] government involvement is needed, its aim should be to support and enforce a predictable, minimalist, consistent and simple legal environment for commerce". [128]

The White House explicitly stated its preference of a self-regulatory approach: "[Governments] should encourage industry self-regulation wherever appropriate and support the efforts of private sector organizations to develop mechanisms to facilitate the successful operation of the Internet. Even where collective agreements or standards are necessary, private entities should, where possible, take the lead in organizing them."[129] Furthermore, it announced to enforce this approach to privacy regulation in international discussions with its most important trading partners like the EU. "To ensure that differing privacy policies around the world do not impede the flow of data on the Internet, the United States will engage its key trading partners in discussions to build support for industry-developed solutions to privacy problems and for market driven mechanisms to assure customer satisfaction about how private data is handled."[130]

The objective of these negotiations was to "bridge the gap" with a solution that would ensure the European requirement of adequacy in regard to protection of personal data from European citizens as well as taking the US American preferred reliance on market mechanisms and self-regulation into account.[131]

The delegation of the Department of Commerce proposed a "Safe Harbor" arrangement, whereby U.S. companies could comply with the directive by agreeing to abide by a list of privacy principles that both the U.S. Government and the EU found acceptable.[132]

The Department of Commerce held hearings of several big international companies and other stakeholders to investigate how proposed draft Safe Harbor regulations would affect their business.

The heard companies pursued two main lines of argument in their comments.

- The European model is considered to be an obstacle for economy and innovation.
- The self-regulatory US solution is considered perfectly adequate and more efficient and appropriate taking into account the innovative capacity of US companies.

Particularly critical in respect to the European comprehensive regulations was Visa. The company considered similar data protection laws in the USA as "a weapon to impair the competiveness of U.S. businesses that have invested heavily in information technologies and are now legitimately reaping the rewards of those investments".[133] "[U]ndue restrictions on

[125] Estimated trade value in year 2000, Schriver 2002, 2779.

[126] Boyd, *Financial Privacy in the United States and the European Union: A Path to Trans-Atlantic Regulatory Harmonization*, 2005, 80.

[127] White House, *A Framework for Global Electronic Commerce*, 1997.

[128] White House 1997.

[129] White House 1997.

[130] White House 1997.

[131] Kobrin, *Safe harbours are hard to find: the trans-Atlantic data privacy dispute, territorial jurisdiction and global governance*, 2004, 120.

[132] Lukas, *Safe Harbor or Stormy Waters? Living with the EU Data Protection Directive*, 2001, 11.

[133] Visa 1999.

the flow of information to and among U.S. companies [...] could have devastating consequences for the U.S. economy."[134]

The Direct Marketing Association praised the "network of targeted privacy protection laws and segment specific self regulation" in the US, that, "while different than the Europeans, is no less protective of our common goal of personal privacy protection".[135]

This very positive view was shared by the US Chamber of Commerce. The Chamber also left no doubt that a self-regulatory solution is the method of choice: "In the United States, industry-wide self regulation of data privacy backed-up by legislation where necessary, has proven to be the most successful and cost effective way to ensure the privacy of consumers."[136]

AT&T, that supported the self-regulatory approach as well, even insisted that they do "not support the concept of financial sanctions or penalties."[137]

"Toward the end of the negotiations, several of the particularly difficult issues were the existence of a public commitment for companies adhering to the code, the access rights and enforcement in the United States. On the US side, the Department of Commerce faced strong pressure from the American business community to block the European Directive. The United States was not prepared to respond to the Directive with new privacy rights and the United States wanted to prevent interruptions in transborder data flows. The Safe Harbor became a mechanism to avoid a showdown judgment on the status of American law and defer action against any American companies."[138]

After long and troubled negotiations[139] the European Commission agreed to endorse the self-commitment of US companies to adhere to this code for personal data of European origin.

Although the European Parliament gave the draft proposal a thumbs down,[140] its rejection was not legally binding, and the European Commission formally certified the Safe Harbor agreement as providing adequate protection on July 26, 2000.[141]

It has to be noted that Safe Harbor is neither a treaty nor an international agreement but rather two unilateral actions: the US issued the principles and the Commission issued an Article accepting them.[142]

5.2.3 Content

Although, to be formally correct, Safe Harbor is neither a treaty nor an international agreement but rather two unilateral actions,[143]

- the Department of commerce issuing the principles and
- the European Commission issuing a decision accepting them,

[134] Visa 1999.

[135] Direct Marketing Association 1998.

[136] US Chamber of Commerce 1998.

[137] AT&T 1998.

[138] Reidenberg, *testimony for the Hearing on the EU Data Protection Directive*, March 8, 2001.

[139] Reidenberg, *testimony for the Hearing on the EU Data Protection Directive*, March 8, 2001.

[140] Schriver 2002, 2789.

[141] Commission Decision 95/46!EC of July 26, 2000, art. 5, 2000 OJ (L 215) 7.

[142] Kobrin, 2004, 121

[143] Kobrin, 2004, 121

due to the comprehensibility of the general linguistic usage, the framework will be referred to as the “Safe Harbor Agreement” in this report.

The terms of contract of this agreement consist of the seven Safe Harbor Principles as well as the less known Frequently Asked Questions, which are also binding for the certifying companies.

5.2.3.1 Safe Harbor Privacy Principles

5.2.3.1.1 Notice

"An organization must inform individuals about the purposes for which it collects and uses information about them, how to contact the organization with any inquiries or complaints, the types of third parties to which it discloses the information, and the choices and means the organization offers individuals for limiting its use and disclosure. This notice must be provided in clear and conspicuous language when individuals are first asked to provide personal information to the organization or as soon thereafter as is practicable, but in any event before the organization uses such information for a purpose other than that for which it was originally collected or processed by the transferring organization or discloses it for the first time to a third party"

The Notice Principle consists of six requirements the self-certifying company has to meet:

- The data subject must be notified about the purposes for which personal information is collected and used.
- The data subject must be notified about contact methods to file inquiries and complaints.
- The data subject must be notified about the types of third parties to whom personal information may be disclosed.
- The data subject must be provided with their choices and means of limiting disclosure of their personal data.
- Notice should be provided at the time when information is first collected or shortly thereafter and must be provided before data is processed or disclosed.
- Notice is mandatory in case of use for secondary usage or disclosure to a third party.

These Requirements do not copy verbatim the requirements of the EU Data Protection Directive 95/46/EC. Nevertheless, the Safe Harbor Principle of “Notice” is by and large congruent with Article 10 of the Directive.

5.2.3.1.2 Choice

"An organization must offer individuals the opportunity to choose (opt out) whether their personal information is (a) to be disclosed to a third party or (b) to be used for a purpose that is incompatible with the purpose(s) for which it was originally collected or subsequently authorized by the individual. Individuals must be provided with clear and conspicuous, readily available, and affordable mechanisms to exercise choice.

For sensitive information (i.e. personal information specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or information specifying the sex life of the individual), they must be given affirmative or explicit (opt in) choice if the information is to be disclosed to a third party or

used for a purpose other than those for which it was originally collected or subsequently authorized by the individual through the exercise of opt in choice. In any case, an organization should treat as sensitive any information received from a third party where the third party treats and identifies it as sensitive."

The Choice Principle has three main requirements:

- The data subject must be able to opt-out of third party disclosures.
- The data subject must be able to opt-out of secondary usage of information.
- The data subject must give affirmative consent (opt-in) for the disclosure or use of sensitive information.

Here, the Safe Harbor Principle Choice may fall short of the consent requirements of the EU directive. While Article 7 demands as a rule the data subject's consent, it is controversial whether this consent may be expressed by passivity, like an opt-out solution entails. The Article 29 Working Party concludes the unsuitability of opt-out solutions because "[un]ambiguous consent does not fit well with procedures to obtain consent based on inaction or silence from individuals: a party's silence or inaction has inherent ambiguity".[144]

Nevertheless, the affirmative consent (opt-in) for sensitive data is congruent with Article 8 of the Data Protection Directive that requires "explicit consent".

However, it is quite problematic that neither "Notice" nor "Choice" reflect purpose limitations, data minimization and duration of storage.

5.2.3.1.3 Onward transfer

"To disclose information to a third party, organizations must apply the Notice and Choice Principles. Where an organization wishes to transfer information to a third party that is acting as an agent, as described in the endnote, it may do so if it first either ascertains that the third party subscribes to the Principles or is subject to the Directive or another adequacy finding or enters into a written agreement with such third party requiring that the third party provide at least the same level of privacy protection as is required by the relevant Principles. If the organization complies with these requirements, it shall not be held responsible (unless the organization agrees otherwise) when a third party to which it transfers such information processes it in a way contrary to any restrictions or representations, unless the organization knew or should have known the third party would process it in such a contrary way and the organization has not taken reasonable steps to prevent or stop such processing."

Onward Transfer has one main requirement:

- All third parties to whom data may be transferred must follow the Safe Harbor principles or Data Directive compliant. The same level of protection must be guaranteed no matter how many times data is transferred.

The first party has to ascertain that the recipient guarantees an adequate level of protection. This responsibility for onward transfer sticking to the first party reflects well the responsibilities of the data controller under the Directive 95/46/EC for onwards transfer.

[144] Article 29 Working Party, WP 187, p. 24.

5.2.3.1.4 Security

"Organizations creating, maintaining, using or disseminating personal information must take reasonable precautions to protect it from loss, misuse and unauthorized access, disclosure, alteration and destruction."

- Entities that process data in any stage of its life cycle (collection, use, analysis, storage) must take reasonable measures to protect against data loss, destruction, misuse and unauthorized access.

The efficiency of this principle depends on the interpretation of “reasonable precautions”. Reasonable in this context can be determined by disproportionate costs or efforts. In which way it has to be determined whether precautions are reasonable or not remains unclear. If the self-certifying company itself may decide whether precautions are reasonable the principle might prove to be rather hollow.

It is also questionable whether there are requirements for a breach notification. As Article 4(2) of the Data Protection Directive states: “In case of a particular risk of a breach of the security of the network, the provider of a publicly available electronic communications service must inform the subscribers concerning such risk and, where the risk lies outside the scope of the measures to be taken by the service provider, of any possible remedies, including an indication of the likely costs involved.”

5.2.3.1.5 Data Integrity

"Consistent with the Principles, personal information must be relevant for the purposes for which it is to be used. An organization may not process personal information in a way that is incompatible with the purposes for which it has been collected or subsequently authorized by the individual. To the extent necessary for those purposes, an organization should take reasonable steps to ensure that data is reliable for its intended use, accurate, complete, and current."

Data Integrity must not be confused with the term “data integrity” of IT professionals. In the context of Safe Harbor it has mainly two requirements:

- Data may only be processed or used as it is related and not incompatible to the purposes for which it was originally collected.
- An entity should take reasonable steps to ensure data is accurate, timely and complete

Here it is unclear if the term “incompatible with the purposes for which it has been collected” covers the whole spectrum of purpose limitation and binding the Directive 95/46/EC imposes on data processing. “Not incompatible” seems to indicate more freedom from the original purpose as in its widest interpretation it only forbids data processing which is contradicting the original purpose.

5.2.3.1.6 Access

"Individuals must have access to personal information about them that an organization holds and be able to correct, amend, or delete that information where it is inaccurate, except where the burden or expense of providing access would be disproportionate to the risks to the

individual's privacy in the case in question, or where the rights of persons other than the individual would be violated."

In short, the certified company has to meet two requirements:

- Data subjects must be able to view the information an organization holds about them.
- Data subjects must be able to correct, add to, or delete inaccurate information.

However, this principle is weaker than the European standard for access. Section V, Article V of the 1995/46/EU Data Protection Directive is entitled, The Data Subject's Right of Access to Data. According to directive, "Member States shall guarantee for every data subject the right to obtain from the controller confirmation as to whether or not data relating to him are processed and information at least as to the purposes of the processing, the categories concerned, and the recipients or categories of recipients to whom the data are disclosed;"

Section V Article 12 also requires that each data subject be entitled to obtain from the controller (of information collected about him or her), "as appropriate the rectification, erasure or blocking of data, the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data". Finally, Article 12 basically guarantees "notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with paragraph 2"

The FAQ on Access gravely derogate this European standard by allowing several loopholes.

5.2.3.1.7 Enforcement

"Effective privacy protection must include mechanisms for assuring compliance with the Principles, recourse for individuals to whom the data relate affected by non-compliance with the Principles, and consequences for the organization when the Principles are not followed. At a minimum, such mechanisms must include (a) readily available and affordable independent recourse mechanisms by which each individual's complaints and disputes are investigated and resolved by reference to the Principles and damages awarded where the applicable law or private sector initiatives so provide; (b) follow up procedures for verifying that the attestations and assertions businesses make about their privacy practices are true and that privacy practices have been implemented as presented; and (c) obligations to remedy problems arising out of failure to comply with the Principles by organizations announcing their adherence to them and consequences for such organizations. Sanctions must be sufficiently rigorous to ensure compliance by organizations."

- A recourse mechanism must be in place for data subjects to file complaints, have disputes investigated, and resolved.
- There must be readily available and affordable independent recourse mechanisms by which each individual's complaints and disputes are investigated and resolved by reference to the Principles and damages are awarded where the applicable law or private sector initiatives so provide.[145]
- An entity must have a mechanism to verify that the stated privacy policy and business operations are compliant with the Safe Harbor agreement. Audits should be completed annually. Follow-up procedures for verifying that the attestations and

[145] Boyd 2005, 82.

assertions businesses make about their privacy practices are true and that privacy practices have been implemented as presented.[146]

- It is the obligation and responsibility of the entity to remedy any problems with compliance in a timely fashion.

The enforcement principle poses according to US privacy expert Joel Reidenberg the most significant deviation from European standards.[147] He criticises the enforcement of Safe Harbor as a weakening of "standards for redress of data privacy violations". [148]

Chris Connolly, former chair of the Consumers' Federation of Australia criticised in its 2008 study on Safe Harbor that more than 500 companies failed to select an independent dispute resolution provider.[149] Furthermore, he denounced that Affordability is a major issue.[150] The Safe Harbor FAQ 11 states that 'the recourse available to individuals must be readily available and affordable. He states that two of the often chosen recourse organisations (The American Arbitration Association, AAA, and The Judicial Arbitration Mediation Service, JAMS) fail to be affordable for the average consumer.[151]

5.2.3.2 Frequently Asked Questions

The second part of the Safe Harbor agreement are the United States Department of Commerce's Frequently Asked Questions of July 21, 2000.[152]

These FAQ explain the aforementioned principles in detail and are often criticised for derogating the requirements of the seven principles by leaving several loopholes for the self-certifying companies.

5.2.4 Progression of Safe Harbor

From the very beginning, American companies targeted be Safe Harbor were reluctant to self-certify. In January 2001, six months after the agreement came into effect, only twelve companies had joint the FTC's list. [153] The growth did not accelerate visibly in the first five years of the agreement. Only from 2006 more and more companies enrolled. By today more than 2,500 companies joint the Safe Harbor.

The initial hesitation was based on several reasons as Kobrin stated in 2004: "In general, American firms believe that Safe Harbor goes too far, that implementing it will be too costly, that it might stimulate pressure for similar legislation in the US and that it might subject them to unforeseen liabilities in Europe."*[154]*

[146] Boyd 2005, 82.

[147] See 5.2.6.1 of this document for a more detailed rendition.

[148] Reidenberg, *testimony for the Hearing on the EU Data Protection Directive*, March 8, 2001.

[149] Connolly, The US Safe Harbor - Fact or Fiction?, 2008, p. 8 and 13.

[150] Connolly, 2008, pp. 13.

[151] Connolly, 2008, p. 14.

[152] Please find the FAQ in Annex C of this Document.

[153] Schriver 2002, 2792f.

[154] Kobrin 2004, 121.

Year	Number of Members
Jan 2001	**12**[155]
Aug 2001	**~ 100**[156] (e.g. Procter & Gamble, Microsoft, Intel)
Mar 2002	**168**[157]
May 2003	**338**[158] (only few major multinational companies)
Apr 2005	**706**[159]
Jul 2009	**1440**[160]
2011	**more than 2500**

Table 1: Progression of Safe Harbor

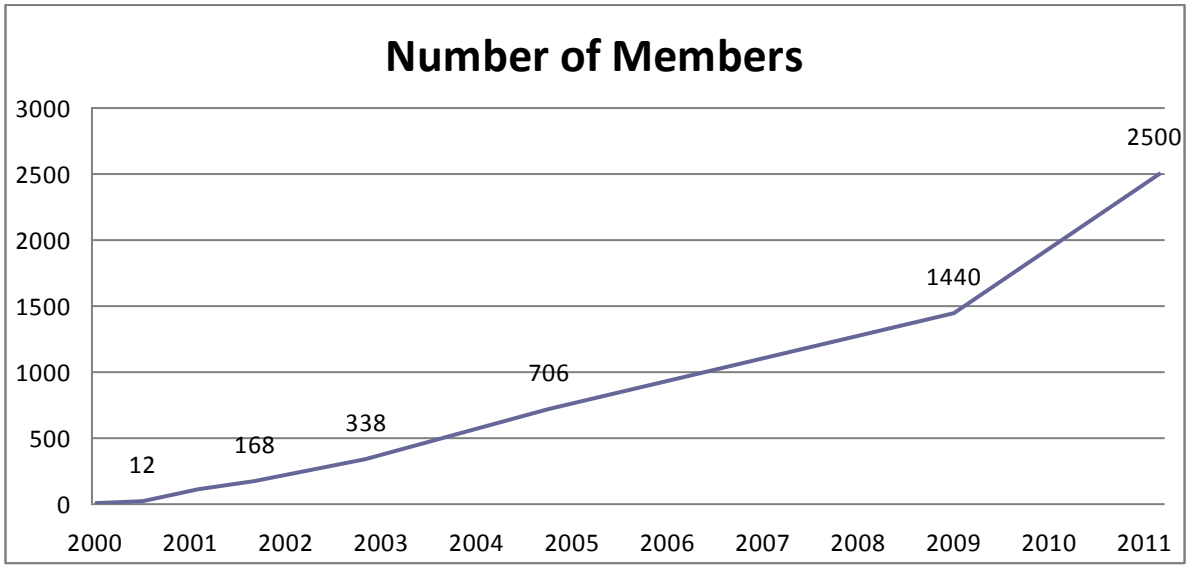


Figure 1: Progression of Safe Harbor

[155] Schriver 2002, 2792.
[156] Schriver 2002, 2792.
[157] Schriver 2002, 2793.
[158] Kobrin 2004, 121.
[159] Boyd 2005, 81.
[160] Takatori 2010, 7.

5.2.5 Enforcement Actions

5.2.5.1 Enforcement 2000-2010

In 2000, after the Safe Harbor Agreement came into effect authorised by the European Commission and the Department of Commerce, a so-called "standstill agreement" became operative.[161] In order to convince the hesitating US companies to certify under Safe Harbor the European Commission refrained from taking enforcement actions until July 1st, 2001. After July, this standstill period was informally prolonged until November.[162] Despite the agreement, in January 2001 only twelve companies had entered the Safe Harbor.[163]

Historically, the Federal Trade Commission (FTC) has done very little to enforce Safe Harbor compliance. Until 2009 the FTC had not commenced a single visible enforcement action in the nine years that the Safe Harbor has been in effect.

However, that began to change in August 2009. Then the FTC publicly announced a suit against the Californian company Balls of Kryptonite, which intentionally misled UK customers to believe it was a European company by using a .co.uk domain address. Furthermore, it claimed in its privacy policy to be Safe Harbor compliant though no certification had ever been registered.[164]

Then, in October 2009, the FTC filed settlement complaints against six multinational companies (World Innovators, Inc.; ExpatEdge Partners LLC; Onyx Graphics, Inc.; Directors Desk LLC; Collectify LLC; and Progressive Gaitways LLC). These companies let their self-certification expire but still claimed to be Safe Harbor compliant in their public privacy policies. Hence, they did not inform the concerned trade partners and data subjects about the change.

For the first time the FTC showed its intention to not longer only rely on self-commitment and regulation by competition to provide adequate enforcement of the Safe Harbor principles. Though the enforcement actions so far are only based on procedural lapse of certification and not on an inspection of the substantive compliance to the principles. Remarkably, these settlements did not include any fines. Instead, the FTC enjoined the concerned companies from any future misrepresentations about their Safe Harbor status.[165] Since the certification requires a public statement in the privacy policy to participate, the FTC had to do nothing more than compare the companies' statements in their privacy policy with the certification records to gain evidence of deceptive trade practices. Hence, these settlements do not reflect the FTC's intention to perform on-site audits to determine whether the company's internal processes for handling personal data actually complies with the seven Safe Harbor principles. [166]

[161] Schriver 2002, 2792.

[162] Schriver 2002, 2792.

[163] Schriver 2002, 2792f.

[164] FTC's press release, August 6th, 2009 http://www.ftc.gov/opa/2009/08/bestpriced.shtm .

[165] Gordon, *Multinationals Certified to the U.S.-E.U. Safe Harbor Agreement Beware: The Federal Trade Commission Has Bared Its Enforcement Teeth*, 2009.

[166] Gordon, 2009.

5.2.5.2 Recent Enforcement

On March 30th, 2011 the FTC announced its first substantive Safe Harbor enforcement action.[167] The settlement order against the social media service Google Buzz represents the first enforcement because of a violation of Safe Harbor principles.

The settlement fits well in the line of the FTC's several actions regarding privacy violations.[168] By Section 5 of the FTC Act the FTC is authorised to take enforcement action against companies engaging in deceptive tactics The Google Buzz settlement, however, is also the first order that requires a company to implement a comprehensive privacy program to protect the privacy of its customers and demands regular, independent privacy audits for the next 20 years.[169]

Google launched its social network Google Buzz in 2010. The company used its customers' lists of email contacts to promote Google Buzz. When the network started, by default, Gmail users became Google Buzz "followers" of their email contacts and were followed by their own contacts as well. Gmail users complained that the automatic generation of follower lists resulted, in some cases, in exposing clients of mental health professionals and attorneys, and job recruiters and users following and being followed by persons against whom they obtained restraining orders or abusive ex-partners.[170]

In the administrative complaint the FTC alleged that Google violated Section 5 of the FTC Act by engaging in deceptive tactics and violating its own privacy policy. Furthermore, the FTC alleged that with respect to the data of its European users, Google failed to adhere to the principles Notice and Choice of the US EU Safe Harbor framework when using its users' information for a purpose different from that for which it was collected, in violation of the company's self-certification.[171]

Notably, an administrative complaint by the FTC is not a finding or ruling that the concerned company has actually violated the law but rather a proceeding when the FTC has "reason to believe" has been violated.[172] Therefore, the FTC may only allege violations of Safe Harbor without a corresponding formal finding. The consent agreement is also for settlement purposes only and does not constitute an admission by Google that the law has been violated. The consent of Google in this settlement, however, indicates that the FTC's allegations were not completely unfounded. The consent agreement carries the law with respect to future actions; violations may result in a civil penalty of up to $16,000.[173]

In detail, in its complaint[174] the FTC alleged that:

- Though the introduction of Google Buzz seemed to offer the user an opt-out choice not to take part in Buzz (e.g. Button "turn off Buzz"), the FTC asserted that an opt-out was actually not possible.

---

[167] Egan, *Google, FTC Reach "Buzz" Settlement*, http://www.insideprivacy.com/united-states/today-the-federal-trade-commission/, 2011.

[168] Segalis, *FTC Takes a Big Step in Privacy Enforcement with Google Buzz Settlement*, http://www.infolawgroup.com/2011/04/articles/enforcement/ftc-takes-a-big-step-in-privacy-enforcement-with-google-buzz-settlement/ 2011.

[169] FTC's press release, March 30th, 2011 http://www.ftc.gov/opa/2011/03/google.shtm.

[170] Egan, 2011.

[171] FTC's press release, March 30th, 2011 http://www.ftc.gov/opa/2011/03/google.shtm.

[172] FTC's press release, March 30th, 2011 http://www.ftc.gov/opa/2011/03/google.shtm.

[173] FTC's press release, March 30th, 2011 http://www.ftc.gov/opa/2011/03/google.shtm.

[174] FTC's complaint in the matter of Google Inc. http://www.ftc.gov/os/caselist/1023136/110330googlebuzzcmpt.pdf.

- Those Gmail users who clicked on the opt-in for Google Buzz were not adequately informed that the identity of individuals they emailed most frequently would be made public by default.
- Google did not provide clear means for users to change privacy settings to prevent the public disclosure of this information.
- The launch of Google Buzz resulted in the disclosure of personal information that was contrary to the users' specific settings (e.g. if a Gmail user blocked another individual from Google Chat, that individual could still be a follower on Buzz). Further, Buzz users did not have the possibility to block followers who did not have a public Google profile. Finally, a flawed design of the Google Buzz reply mechanism to comments resulted in broad disclosure of users' private email addresses.[175]

Jon Leibowitz, Chairman of the FTC has labelled this enforcement action a "tough settlement that ensures that Google will honor its commitments to consumers and build strong privacy protections into all of its operations". [176]

The consent settlement[177] between the FTC and Google includes several major requirements:

- It demands Google to grant its users Notice and Choice prior to disclosing their personal information to third parties.[178] It requires Google to give users a clear notice of the proposed disclosure of personal data and to obtain their "express affirmative consent".[179] Although the settlement does not define "express affirmative consent", at a minimum, this provision will demand Google to offer its users a prominent, transparent means for exercising their privacy choices.[180]
- It requires Google to establish and implement, and thereafter maintain a comprehensive privacy program.[181] The program has to include the privacy controls and procedures appropriate to the company's size and complexity, the nature and scope of its processing activities, and the nature of the covered personal data. It has to be reasonably designed to
    - address privacy risks related to the development and management of new and existing products and services, and
    - protect the privacy and confidentiality of the covered information.[182]

  Including this requirement appears to be the first application of the "privacy by design" approach that the Commission articulated in its Privacy Report in December 2010.[183] The FTC's "privacy by design" approach calls on companies to integrate substantive

[175] Egan, 2011.

[176] FTC's press release, March 30th, 2011 http://www.ftc.gov/opa/2011/03/google.shtm.

[177] FTC's agreement containing consent order in the matter of Google Inc., File No. 102 3136, http://www.ftc.gov/os/caselist/1023136/110330googlebuzzagreeorder.pdf.

[178] Egan, 2011.

[179] FTC's agreement containing consent order in the matter of Google Inc., File No. 102 3136, p. 4, http://www.ftc.gov/os/caselist/1023136/110330googlebuzzagreeorder.pdf.

[180] Egan, 2011.

[181] FTC's agreement containing consent order in the matter of Google Inc., File No. 102 3136, p. 4, http://www.ftc.gov/os/caselist/1023136/110330googlebuzzagreeorder.pdf.

[182] Egan, 2011.

[183] FTC, *Protecting Consumer Privacy in an Era of Rapid Change – a Proposed Framework for Business and Policymakers*, 2010, p. v, ix, http://www.ftc.gov/os/2010/12/101201privacyreport.pdf.

technical and organisational privacy protection measures into their business practices, such as data security, reasonable collection limits, sound retention practices, and data accuracy.[184] This includes that companies should maintain comprehensive data management procedures throughout the life cycle of their products and services. The report also called for companies to implement procedurally adequate privacy practices throughout the organisation, including assigning personnel to oversee privacy issues, training employees and conducting privacy reviews for new products and services.[185]

- Finally, the consent order requires Google to verify its implementation and adherence to this comprehensive privacy program by obtaining initial and biennial assessments and reports from a qualified, objective, independent third-party professional for the next 20 years.[186]

5.2.5.3 Evaluation of Enforcement Actions

Though in the first nine years of the Safe Harbor Agreement the FTC seemed reluctant to take any visible Section 5 enforcement actions against companies misrepresenting Safe Harbor compliance, the recent two years reveal a different picture. Especially the complaint and consent order against Google Inc. showed that the FTC is willing and able sanction severe violations of consumer privacy with considerable penalties. After the first complaints in 2009 because of lapse in self-certification, the Google Buzz settlement seems to be an action “pour encourager les autres”.

Although the conditions of the consent order might seem to be harsh (especially the requirement for biennial audits over the next 20 years) compared to the prior Safe Harbor violation complaints and settlements, it must not be forgotten that the Google Buzz complaint did not solely base on a Safe Harbor violation.

It remains to be seen if the FTC will keep up its hard line when dealing with companies that “only” violate Safe Harbor principles.

Nevertheless, the impact of the Google Buzz settlement on other self-certified companies as well as the FTC’s Privacy by Design approach are most welcome in regard to the future development of Safe Harbor.

5.2.6 Criticism of Safe Harbor

Since the Safe Harbor Agreement came into effect, it was criticised from both sides of the Atlantic. The US side criticised that the principles are too restrictive and cost intensive. The EU side criticised the lack of adequacy in data protection standards.

The European Commission published two working papers in 2002 and 2004/5 evaluating Safe Harbor.

The working paper issued in early 2002 diplomatically expressed serious concerns about the adequacy of data protection as well as the actual implementation. It states that out of the few self-certified companies many do not meet the requirements of the Safe Harbor Principles. The working paper concluded, “that a substantial number of organisations do not meet the

[184] FTC, Protecting Consumer Privacy in an Era of Rapid Change – a Proposed Framework for Business and Policymakers, 2010, p. ix, http://www.ftc.gov/os/2010/12/101201privacyreport.pdf.

[185] Egan, 2011.

[186] FTC’s agreement containing consent order in the matter of Google Inc., File No. 102 3136, p. 5, http://www.ftc.gov/os/caselist/1023136/110330googlebuzzagreeorder.pdf.

requirement that they publish a compliant privacy policy and indicate publicly their adherence to Safe Harbor. Less than half of those organisations post privacy policies that reflect all seven Safe Harbor principles or inform individuals how they can proceed with complaints and a dispute resolution mechanism."[187] The report furthermore criticises that none of these companies has been prosecuted by the FTC for making false statements.

Four years after the implementation of Safe Harbor, the Commission issued a second working paper reviewing the adequacy of the Safe Harbor programme.[188] The Commission still found a substantial number of companies fail to publish publicly available privacy policies. Out of the publicly available ones many policies failed to clearly describe processing operations or the access right of the data subject. Some companies failed to give data subjects the opt-out choice in regard to data disclosure to third parties. And lastly, a substantial number of companies did not identify arbitration boards or other entities to resolve the data subject's complaints. "These shortcomings are serious; unless safe harborites publish appropriate privacy policies, the US Federal Trade Commission […] which is responsible for enforcing Safe Harbour is unable to take enforcement action."[189]

As a result the Commission recommends the FTC to give guidance to the self-certifying companies on what qualifies a publicly available privacy policy. Furthermore, the Commission urges the FTC to take a more active role in enforcing the compliance with the Safe Harbor Principles.

Besides these findings of the European Commission, there are several targets of severe criticism of Safe Harbor.

5.2.6.1 Weakening of European Standards

US privacy expert Joel Reidenberg stated that Safe Harbor constitutes "a weakening of European standards". [190]

Especially remarkable are the allowed exceptions from Safe Harbor with significant loss of coverage for specific categories of data. "The Safe Harbor exempts public record information despite its ordinary protection under European law. Similarly, the Safe Harbor exempts any processing pursuant to any 'conflicting obligation' or 'explicit authorization' in US law whether or not such processing would be permissible under European standards." [191]

Additionally, the Access Principle includes derogations that do not exist in Article 12 of the Data Protection Directive.

The most significant deviation according to Reidenberg lies in the weakening of "standards for redress of data privacy violations". [192] In Chapter III of the Data Protection Directive "judicial remedies, liability and sanctions" the Directive guarantees the victim remedy for any breach of the rights guaranteed him. During the Safe Harbor negotiations the Department of Commerce assured the Commission that the US judiciary provides sufficient remedies for

---

[187] Kobrin 2004, 122.

[188] European Commission Staff Working Document: The implementation of Commission Decision 520/2000/EC on the adequate protection of Personal data provided by the Safe Harbour privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce. SEC (2004) 1323. October 20, 2004, at 105.

[189] http://www.twobirds.com/German/News/Articles/Seiten/EU_Commission_critical_of_US_Safe_Harbor_programme.aspx .

[190] Reidenberg, *testimony for the Hearing on the EU Data Protection Directive*, March 8, 2001.

[191] Reidenberg, *testimony for the Hearing on the EU Data Protection Directive*, March 8, 2001.

[192] Reidenberg, *testimony for the Hearing on the EU Data Protection Directive*, March 8, 2001.

European victims of breaches of Safe Harbor violations. Reidenberg criticises that these assurance was misleading: "For example, the memorandum provides a lengthy discussion of the privacy torts and indicates that the torts would be available. The memorandum failed to note that the applicability of these tort actions to data processing and information privacy has never been established by US courts and is, at present, purely theoretical. Indeed, the memorandum cites the tort for misappropriation of a name or likeness as a viable damage remedy, yet all three of the state courts that have addressed this tort in the context of data privacy have rejected it."[193]

Additionally, the arbitration boards intended for the predicated dispute resolution lack in regard to offering a direct remedy to the victim. [194]

5.2.6.2 Limited Applicability

Criticism has also been levelled at the narrow applicability of Safe Harbor. First, Safe Harbor by its terms can only apply to US organisations that fall within the regulatory jurisdiction of the FTC and the Department of Transportation. Therefore, many sectors are ineligible for Safe Harbor certification. Expressly excluded from the FTC's jurisdiction are

- financial institutions, including banks, savings and loans, and credit unions,
- telecommunications and interstate transportation common carriers,
- employment sector,
- air carriers and
- packers and stockyard operators.[195]

Another problem is that even if a company falls under the jurisdiction of the FTC and certifies as Safe Harbor compliant it may have limited the scope of its Safe Harbor membership to specific categories of data. It is possible to restrict the applicability to e.g. Human Resources data, online data, or other specific categories. This introduces further gaps in the protection framework of Safe Harbor. A European data controller has to verify for each occurring data transfer to a Safe Harbor company if the certification applies to the concerned category of data.

5.2.6.3 Dubious Legality

The legality of the unilateral actions of the Department of Commerce and the European Commission was questioned since the implementation of Safe Harbor.

Short time after the hearings, Rick Lane, director of E-Commerce and Internet Technology at the U.S. Chamber of Commerce, went so far as to say that the Department of Commerce never had the authority to negotiate the deal in the first place.[196]

Regarding Europe similar doubts on level of procedural law were being voiced. Reidenberg pointed out, that the decision on the approval of Safe Harbor by the European Commission was made before Safe Harbor was in existence.[197] This contradicts the requirements of the

[193] Reidenberg, *testimony for the Hearing on the EU Data Protection Directive*, March 8, 2001.

[194] Reidenberg, *testimony for the Hearing on the EU Data Protection Directive*, March 8, 2001.

[195] http://www.export.gov/safeharbor/eu/eg_main_018481.asp .

[196] Carlson, *U.S. Firms Find No Haven in Safe Harbor*, 2001, 37.

[197] Reidenberg, *testimony for the Hearing on the EU Data Protection Directive*, March 8, 2001.

Data Protection Directive that “adequacy” has to be assessed in light of the prevailing “rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country”.[198] Safe Harbor was not “in force” at the time of the Commission’s decision. The European Parliament referred to this problem shortly before the Commission’s approval without any further impact on the decision.[199]

Furthermore, according to the directive, the European Commission only has authority to enter into negotiations to remedy the absence of “adequate” protection after a formal finding that the non-European country fails to provide “adequate” protection.[200] But in case of the USA the Commission never made this formal finding.[201]

Both activities appear to be “significant administrative law defects”.[202] “Although the European Commission maintains that the European Parliament did not say that the Commission acted outside its powers and the Member States voted unanimously in the political committee to accept the Safe Harbor, this administrative process problem remains an open question that only the European Court of Justice can resolve and gives the independent national supervisory authorities grounds to vitiate Safe Harbor through strict interpretations of the European Commission’s ruling.” [203]

In addition, the European Parliament pointed out: “The risk that the exchange of letters between the Commission and the US Department of Commerce on the implementation of the 'safe harbour' principles could be interpreted by the European and/or United States judicial authorities as having the substance of an international agreement adopted in breach of Article 300 of the Treaty establishing the European Community and the requirement to seek Parliament's assent (Judgment of the Court of Justice of 9 August 1994: French Republic v. the Commission -- Agreement between the Commission and the United States regarding the application of their competition laws (Case C-327/91))”[204]

5.2.6.4 Lack of Enforcement

Lastly and most seriously the enforcement provisions of the FTC have been criticised.[205] Because Safe Harbor relies on a system of self-certification the enforcement of compliance turns out to be conditio sine qua non for the efficiency of data protection under the Safe Harbor Framework.

The “less than aggressive” enforcement actions from 2000 until 2009 were raising doubts on the willingness of the FTC to enforce the Safe Harbor Principles at all. The most severe criticism was voiced by former Chair of the Consumers' Federation of Australia Chris Connolly in 2008.[206] The study assessed the compliance of self-certified companies with Safe Harbor principle 7 “Enforcement”. Connolly found that out of 1,597 companies claiming

[198] 95/46/EC Article 25 Paragraph 2.

[199] Reidenberg, *testimony for the Hearing on the EU Data Protection Directive*, March 8, 2001.

[200] 95/46/EC Article 25 Paragraph 5.

[201] Reidenberg, *testimony for the Hearing on the EU Data Protection Directive*, March 8, 2001.

[202] Reidenberg, *testimony for the Hearing on the EU Data Protection Directive*, March 8, 2001.

[203] Reidenberg, *testimony for the Hearing on the EU Data Protection Directive*, March 8, 2001.

[204] European Parliament Resolution A5-0177/2000 on the Draft Commission Decision 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 (C5-0280/2000 - 2000/2144(COS)) (July 5, 2000) , § E(2).

[205] Ninja Marnau, Eva Schlehahn, *Cloud Computing und Safe Harbor*, DuD 5/2011, p. 314

[206] Connolly, The US Safe Harbor - Fact or Fiction?, 2008.

to be Safe Harbor compliant only 348 were actually formally compliant with the requirements of the principle "Enforcement".

The following table[207] shows the study's results in detail:

Membership Requirement	Notes	Number of entries	Number of unique entries removed	Total
Organisation is listed	All organisations listed on 17 October 2008.	1597	0	**1597**
Unique entry	Removes doubles, triples and the test file	19	19	**1578**
Collects EU personal information	Removes irrelevant organisations who do not collect any EU personal information	7	7	**1571**
Listed as current by DOC	Removes organisations listed by the Department of Commerce as 'not current'	342	329	**1242**
Listed as current by certification renewal date	Removes organisations that failed to renew by 17 October 2008.	477	133	**1109**
Website privacy policy is accessible	Removes organisations who claim to have a website privacy policy, but it is unreachable.	175	57	**1052**
Privacy policy mentions Safe Harbor	Removes organisations who have a public privacy policy but it does not mention the Safe Harbor at all	218	127	**925**
Privacy policy complies with the enforcement principle	Removes organisations who have a public privacy policy that does not provide information on the selected dispute resolution provider.	587	279	**646**
Affordable dispute resolution provider	Removes organisations who have selected AAA or JAMS as their dispute resolution provider in either their certification record or their public privacy policy.	209	107	**539**
Verified member of TRUSTe dispute resolution.	Removes organisations who have selected TRUSTe as their dispute resolution provider when they are not current members.	29	11	**528**

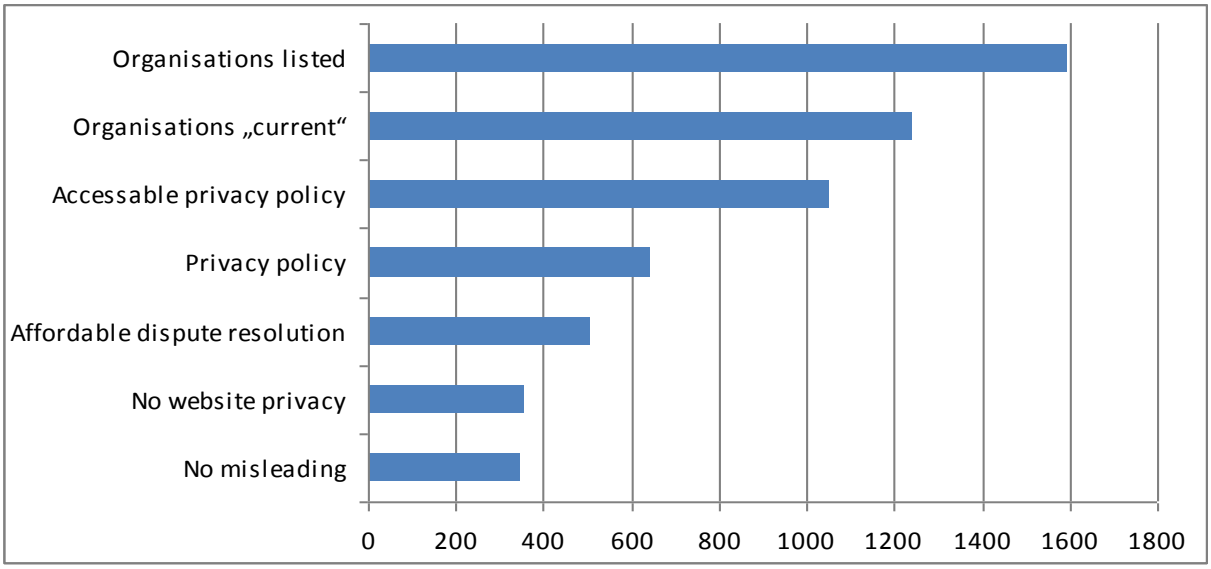
[207] Connolly, 2008, pp. 7-8.

Membership Requirement	Notes	Number of entries	Number of unique entries removed	Total
Verified member of TRUSTe privacy program	Removes organisations who claim to be members of the TRUSTe privacy program when they are not current members	30	2	**526**
Verified member of the BBB Safe Harbor program	Removes organisations who claim to be members of the BBB Safe Harbor program when they are not current members.	4	3	**523**
Dispute resolution provider exists	Removes organisations who have selected BBB Online Privacy as their dispute resolution provider (closed in July 2008)	21	15	**508**
Privacy program exists	Removes organisations who claim to be members of BBB Online Privacy (closed in July 2008)	31	3	**505**
No website privacy policy	Removes organisations who require a password or direct contact in order to obtain their privacy policy.	246	151	**354**
No misleading information	Removes organisations who are using unauthorised Safe Harbor seals or who claim they have been certified by the Department of Commerce or the EU	32	6	**348**

Table 2: Lack of Enforcement – Study

Especially the high number of companies not making their privacy policy publicly available is remarkable. Equally alarming is the number of privacy policies that did not provide information on the selected dispute resolution provider.

The following diagram shows the vast discrepancy between the overall numbers of listed companies to the number of companies formally compliant to the enforcement requirements.



Moreover, despite these remaining 348 companies were found to be formally compliant with principle 7, Connolly warns that they might not be compliant with all seven of the more detailed Safe Harbor Principles.[208]

Although the test criteria of Connolly might be criticised, his results were alarming. Despite the fact that the FTC had to do nothing more than to check the self-certifying company's publicly available privacy policy, 477 certifications were out of date, 246 privacy policies were not publicly available and 587 companies failed to mention a civil dispute resolution organisation.

The most recent settlement in 2009 and with Google Inc. in 2011 might silence part of this criticism, if the FTC continues its enforcement of Safe Harbor principles. Nevertheless, in more than 10 years of Safe Harbor there have been no fines for violation of Safe Harbor.

5.2.7 Political Reactions and Outlook

Although Safe Harbor was criticised by European privacy experts since it came into force, neither on EU level nor on national level there have been any decisions regarding a possible insufficiency of Safe Harbor.

After the Galexia Study "The US Safe Harbor – Fact or Fiction?" by Chris Connolly, data privacy and consumer protection activist and Member of the Management Board of the Australian Privacy Foundation, was published in 2008[209], the European suspicion against Safe Harbor grew.

In 2010 the informal coordinating body of the German data protection authorities (Düsseldorfer Kreis), stated in a formal decision that German companies must not rely blindly on the compliance of US companies who claim to be self-certified under Safe Harbor. They have to check minimum criteria in advance to lawfully transfer data. The German company has to verify if the Safe Harbor self-certification is valid and if the recipient fulfils its duties in regard to the principles "Notice" and "Choice". This decision states more or less a

[208] Connolly, 2008, p. 8.

[209] Connolly, 2008.

renunciation of Safe Harbor reliance for German companies. However, it remains to be seen if this decision of the German data protection authorities will be upheld by the courts.

The German Government does not see any need for them to take action with regard to the US-American "Safe Harbor" framework. In a response to a query made by the SPD parliamentary group dated 25 October 2010 the Government refers the issue to the European Commission and the supervisory authorities of the German States. Nevertheless, the 1995 EU Data Protection Directive will be reconsidered in 2011. In this context the European Commission will also revise the Safe Harbor Agreement.

In its resolution of 6 July 2011 on a comprehensive approach on personal data protection in the European Union (2011/2025(INI)) the European Parliament calls on the European Commission to assess carefully the effectiveness and correct application of the Safe Harbour Principles.[210] It is to be expected that the outcome of this long overdue revision of Safe Harbor will have serious impact on the EU-US data flows. It is to be expected that the criticism of the Galexia Study as well as the decision of the Düsseldorfer Kreis will have serious impact on this revision.

5.2.8 Safe Harbor: Conclusions in regard to Cloud Computing

It would not be too farfetched to state that Safe Harbor was more of a political decision than an actual adequacy finding based on facts. The sustainability of Safe Harbor is questionable as permission for the transfer of personal data by European companies. The German Data Protection Authorities decided on mandatory additional measures and contracts to validate and safeguard the adequacy of the data protection standard within the Safe Harbor self-certified US company. For German data controllers the advantages und simplifications of Safe Harbor are more or less annulled. Although other EU member states have not explicitly stated similar additional requirements for the data transfer, the suspicion towards Safe Harbor is growing within the EU.

In its resolution of 6 July 2011 on a comprehensive approach on personal data protection in the European Union (2011/2025(INI)) the European Parliament calls on the European Commission to assess carefully the effectiveness and correct application of the Safe Harbour Principles.[211] It is to be expected that the outcome of this long overdue revision of Safe Harbor will have serious impact on the EU-US data flows.

Considering the market leadership of US Cloud Service Providers this will also have a great impact on cloud computing customers in Europe. At the moment, apart from Germany with its additional requirements, Safe Harbor is in a merely formal sense a lawful legitimation of European data controllers to commission US CSP with the processing and storing of personal data. But as there are considerable consequences of the revision to be expected within the next year, European cloud customers should revert to more sustainable contractual solutions. Due to the valid criticism this additional safeguarding should also be in their interests. Solutions could be the commissioning of a completely European CSP as well as the use of Standard Contract Clauses or Binding Corporate Rules for commissioning a US CSP. The evaluation of the effectiveness of Standard Contract Clauses and Binding Corporate Rules will be part of R1.2.1.4.

---

[210] European Parliament resolution of 6 July 2011 (2011/2025(INI), Nr. 47 http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2011-0323+0+DOC+XML+V0//EN

[211] European Parliament resolution of 6 July 2011 (2011/2025(INI), Nr. 47 http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2011-0323+0+DOC+XML+V0//EN

5.3 Territorial restrictions on data transmissions

Apart from the issue of adequate level of protection to make the disclosure of personal data legitimate, many countries have specific regulations in certain areas that need to be taken into account to ensure the lawfulness of the data processing in question. So for instance, the transmission of certain data types may be forbidden. Also, the usage of cloud solutions may be prohibited for certain potential user groups. This is not only a problem within the European Area but also in international context outside EU. So for example, Canada's Bank Act states under its subsection "Requirement to maintain copies and process information in Canada" in Article 245 (1), that banks are required to maintain and process data solely in Canada. This encompasses information or data concerning the preparation and maintenance of bank records and central security registers, including customer account records. An exemption of this prohibition can only be made if the bank applied for and received approval of the Office of the Superintendent of Financial Institutions (OSFI). This is due to the USA PATRIOT Act, which allows the FBI and other agencies the access to data stored on any computer located in the U.S. even if it is being hosted on behalf of another sovereign state.[212] As a consequence, the Dutch government intends to rule out US providers out of contracts due to privacy concerns related to the personal data of its citizens.[213] However, the United Kingdom has an authorisation of its governmental agencies similar as the US Patriot Act written into in its Regulation of Investigatory Powers Act.[214] Therefore, cloud hosting services in the US or United Kingdom may not be the ideal IT solution not only for the banking sector in Canada. Consequently, government ministers of France are not allowed to use Blackberry's due to the accessibility of data stored in data centres in the US and UK.[215] Another uncertainty is if these executive powers even extend over data that is hosted at a legal subsidiary of a US or UK located parent company. In the US, a considerable hurdle for using cloud computing services does exist in the health sector. The US Health Insurance Portability and Accountability Act (HIPAA) has strict requirements in respect to supervision and auditing of health records, which may cause severe factual problems for data stored and processed in an cloud environment.[216] Similarly, the US Sarbanes Oxley Act (SOX) imposes very strict documentation and disclosure obligations on companies, which are difficult to fulfil if the company has no direct influence on the means of the data processing within the cloud.[217] All of these restrictions on data processing are significant obstacles for the usage of cloud computing and clearly indicate that a more comprehensive protection of the data supposed to get transmitted across borders is needed.

[212] See for instance, the Articles of Title II USA PATRIOT Act (Enhanced surveillance procedures). The extension of the USA PATRIOT Act until December 2013 is currently undergoing discussion in the government. On February 27th 2011, President Barack Obama signed a temporarily extension of three controversial provisions of the Patriot Act that had been set to expire by the end of the month.

[213] Zack Whittaker, *Dutch government to ban U.S. providers over Patriot Act concerns*, published 19 September 2011, see also Whittaker, *Patriot Act affects European cloud adoption*, published 2 August 2011.

[214] Notable is especially Part III of the Regulation of Investigatory Powers Act (Investigation of electronic data protected by encryption etc.), which obligates persons to provide a decrypted version and/or the cryptographic key of previously encrypted data to government representatives.

[215] BBC News of Wednesday, 20 June 2007, http://news.bbc.co.uk/2/hi/business/6221146.stm .

[216] Cf. especially the regulations under Title II HIPAA: Preventing Health Care Fraud and Abuse; Administrative Simplification.

[217] Cf. the regulations under Title III (Corporate Responsibility) and Title IV (Enhanced Financial Disclosures) of the SOX.

Chapter 6

Cloud Computing: Methods of resolution

This section will address tangible measures to approach the above elucidated problems related to cloud computing. It will analyse some concepts and developments in the legal, contractual and technical field that may potentially qualify as adequate solutions for some of these critical issues in respect to European data protection.

6.1 Legal

As we already discussed in the above sections, the identification of involved parties, the allocating the corresponding legal responsibilities and enforcing the compliance with data protection requirements are the main issues in a cloud computing context. In this subsection, we will introduce potential approaches to these issues and discuss their suitability for problem solution.

6.1.1 Identifying the involved

The EU Data Protection Directive differs between data controllers and data processors to determine the legal responsibility for the processing of personal data. This responsibility lies within the sphere of the controller of the processing. But a precondition for the determination who is controller and who is processor is that the parties involved are known. So they need to get identified first. Hence, the identification of the stakeholders for each action within the cloud service provision and consumption is crucial for any responsibility allocation. Cloud computing nowadays comes with the most different models of service provision. For instance, the services can be delivered within federated cloud architectures, multi-provider-hosting, multi-cloud architectures and hybrid clouds.[218] These different delivery types mainly take the provider side into account. Still, the all-embracing consideration of all possible parties involved is important as a first, indispensable step to enable a comprehensive allocation of the legal responsibilities for any operations done in the cloud context.[219]

[218] The legal assessment of Barnitzke et al. for the EU-funded Optimised Infrastructure Services (OPTIMIS) project provides an in-depth analysis of these different models and their impact on the responsibility allocation in its Deliverable D7.2.1.1 – Cloud Legal guidelines, p. 43 ff.

[219] In Annex A to this document, we provide an exemplary role model that breaks down und further details possible roles of involved parties, depending on the specific real-life context. This also conveys the identification of the specific key stakeholders for each individual service and operation related to the cloud environment to enable an allocation of legal responsibilities in a second step. Still, this role model may be not conclusive and suitable for all thinkable constellations that may occur. According to the EU Data Protection Directive 95/46/EC, whoever has the direct authority and factual control to initiate and determine a decision about the processing of personal data must be regarded as a controller responsible for the lawfulness of the data processing. Hence, an exhaustive assessment of the factual situation and the level of control a party has must be made.

6.1.2 Allocating responsibilities

According to the Directive, it is the controller, who is responsible for the lawfulness of the data processing in terms of data protection law. Therefore the determination who is controller during a data processing is of significance for the allocation of the legal responsibility. The accountability of a service provider is of crucial importance for the trust into the business model cloud computing. Corresponding to this, the Centre for Information Policy Leadership as Secretariat to the Galway Project defined five key elements of accountability. These elements are:

- Organisation commitment to accountability and adoption of internal policies consistent with external criteria
- Mechanisms to put privacy policies into effect, including tools, training and education
- Systems for internal, ongoing oversight and assurance reviews and external verification
- Transparency and mechanisms for individual participation
- Means for remediation and external enforcement[220]

The demand and benefits of accountability result from the clarity of abstract commitment as well as from tangible roles, working fields and realisation mechanisms. Thus, these elements are useful to give a practicable conception for accountability. Moreover, in the follow-up Paris project, criteria for the demonstration of accountability were identified. These serve as definition frame and cover the following questions:

- For What Are Organisations Accountable?
- To Whom Are Organisations Accountable?
- Common Fundamentals of an Accountability Implementation Program, such as
    - Policies
    - Executive Oversight:
    - Staffing and Delegation
    - Education and awareness
    - Ongoing risk assessment and mitigation
    - Program risk assessment oversight and validation
    - Event management and complaint handling
    - Internal enforcement
    - Redress[221]

[220] Centre for Information Policy Leadership as Secretariat to the Galway Project, *Data Protection Accountability: The Essential Elements, A Document for Discussion*, October 2009, p. 17 f. The Galway project is an initiative founded and fostered by Ireland's Office of the Data Protection Commissioner and co-sponsored by the OECD. It focuses on questions of responsibility and reliability in terms of data protection in respect to the rapidly progressing development and complexity of international data transfers

[221] Centre for Information Policy Leadership as Secretariat to the Paris Project, *Demonstrating and Measuring Accountability – A Discussion Document, Accountability Phase II – The Paris Project*, October 2010, p. 5 ff.

Taking these criteria into account, the consequence in respect to cloud computing must be a case-by-case assessment with a closer inspection of the situation in question. Even though the customer would be in most cases the controller of the data processing (and thus the legally responsible party) with the provider as his processor acting only on his behalf, the factual control over the processing often lies within the sphere of the service provider. This means in regard to cloud computing, that the situational control of the CSP needs to be analysed and its relevance for the processing of the personal data determined. Due to the fact that in most cases, the customer will not be able to visit the data centres himself to overview the means of the processing, CSP's should aim at achieving more transparency in regard to their work. This refers to better and clearer content and wording of data protection policies as well as to more refined and consumer-friendly SLA's. On consumer side, it is advisable to perform a comprehensive and context-tailored risk assessment in advance of the service usage to meet the legal responsibility compliant to the requirements of the EU Data Protection Directive. The European Network and Information Security Agency (ENISA) provide some guidance via its Cloud Computing Security risk assessment, which may be a good start to begin with. This analysis introduces some helpful use case scenarios and identifies the specifically cloud-related risks, such as policies and organisational risks (like vendor-lock-in, compliance issues) as well as technical and legal risks.[222] Still, a more detailed assessment tailored to the specific needs of the potential consumer may most advisable to avoid unexpected risks in advance.

6.1.3 Enabling Enforcement

The deficits of the current legal data protection framework lie within the limited power of the European data protection supervisory authorities and the lack of precise legal provisions for compliance auditability as well as for data breach handling in general. All these issues are currently being discussed and approached on European level as well as on national level. Neelie Kroes, European Commission Vice-President for the Digital Agenda, highlighted in her speech of 25 November 2010 about cloud computing, that every potential customer of a cloud service should have knowledge how his provider protects the personal data entrusted to him and if the service is compliant with the European data protection law. Furthermore, governments shall be able to ensure the adequate protection of that personal data via effective legal frameworks. To achieve this, the EU Data Protection law is currently undergoing revision. First results are expected to be published by the end of 2011.[223] Part of the revision process is a public consultation that was launched by the European Commission in May 2009. This consultation focused on current issues in regard to the legal framework for the fundamental right to protection of personal data in the EU and desirable changes to improve this framework. The consultation was concluded in December 2009 and showed that the relevant stakeholders (citizens, organisations and public authorities) expressed strongly the necessity of a modernisation of the current data protection legislation in Europe to meet the challenges of new technologies.

Also, the Article 29 Data Protection Working Party issued a statement, highlighting that the Lisbon extension of EU data protection law to the former third pillar call for improvement,

[222] European Network and Information Security Agency (ENISA), *Cloud Computing - Benefits, Risks and Recommendations for Information Security*, published 20 November, 2009, p. 21 ff.; This risk assessment guidance was also recommended by the Danish DPA in its Opinion: *Regarding processing of confidential and sensitive personal data in connection with use of Google Apps online office suit* of 3 February 2011, p. 3

[223] Neelie Kroes, European Commission Vice-President for the Digital Agenda, *Cloud Computing and Data Protection*, Les Assises du Numérique conference, Université Paris-Dauphine, 25 November 2010

clarification and innovation of the current legislation.[224] The Article 29 working party press release of 11 April 2011 stated that it is going to prepare itself to address law enforcement issues in the near future to contribute to a comprehensive data protection legal framework.[225]

In April 2010, an expert group was established to assist the European Commission in achieving a further development of European contract law. Within this context, this expert group submitted a feasibility study, which covers the most relevant practical issues in a contractual relationship, such as legal rights for faulty goods and rules on which contract terms may be unfair. The results of the study will be of influence to the future approach of the European Commission in further developing the European contract law.[226]

Viviane Reding, Vice-President of the European Commission and EU Justice Commissioner, drew particular attention to the fact that the rapid technological changes of today's world are a challenge for the protection of fundamental rights, including the protection of personal data. Part of this challenge is the enforcement of the protection requirements. Hence, the review of the European data protection framework shall include the enforcement issue in the 27 EU member states by further harmonising the powers of European data protection authorities. Legislative proposals were announced for the end of year 2011.[227] Reding also said in an interview that recent data breach events show that consumers are in need of strengthening their data protection rights. The insufficient data protection measures of service providers lead to a diminishing of consumer's trust and should be restored by the revision of the European data protection framework. This revision is intended to come with stricter regulation in respect to jurisdiction and applicableness of European data protection law and companies' data breach notification obligations.[228]

6.2 Contractual and other regulations

This section will introduce contractual and company-internal instruments to cope with the legal issues of personal data protection in the context of cloud computing business. Such instruments are:

- EU Standard Contractual Clauses (EU SCC)
- Codes of Conduct (CoC)
- Binding Corporate Rules (BCR)

[224] Cf. European Commission, Directorate-General Justice, *Summary of replies to the public consultation about the future legal framework for protecting personal data*, Brussels, 4 November 2010

[225] Article 29 Working Party press release of 11 April 2011 about the 80th plenary meeting on 4 and 5 April 2011 in Brussels

[226] Commission Expert Group on European Contract Law, *Feasibility study for a future instrument in European Contract Law* of 3 May 2011, comprised in the European Commission document "A European contract law for consumers and businesses: Publication of the results of the feasibility study carried out by the Expert Group on European contract law for stakeholders' and legal practitioners' feedback" (Annex IV)

[227] Viviane Reding Vice-President of the European Commission and EU Justice Commissioner, *Your data, your rights: Safeguarding your privacy in a connected world* – speech held at *the* Privacy Platform "The Review of the EU Data Protection Framework" Brussels, 16 March 2011

[228] Viviane Reding, *Companies don't take protection of personal data seriously enough*, an interview on strengthening consumer's data protection rights as consequence of data breach cases of Apple and Sony

In the following subsections, these instruments will be examined in regard to nature, requirements and suitability to solve the issue of implementing effective protection of personal data.

6.2.1 EU Standard Contractual Clauses

The legislative regulation of European data protection enables the transmission of personal data within the area of the European Union. Still, any further disclosure across the borders of the EU/EEA into a third country is not per se covered by such statutory permission. The decisive factor for a lawful disclosure is the existence of an adequate level of protection for the personal data in question. For some countries outside the European Union, this adequate level of protection through legislative measures was acknowledged by the European Commission. Nevertheless, this leaves the question open how such an acknowledgement could be achieved in other countries that do not provide such automatic protection by national law. An instrument to achieve the adequate protection of personal data, compliant with the requirements of the EU Data Protection Directive 95/46/EC, could be the usage of the European Standard Contractual Clauses provided by the European Commission. These complement the contract entailing the primary contractual service agreement and specify them with respect to the European requirements of minimal data protection standards. The possibility of using these clauses is at disposal for European citizens and organisations due to the principle of freedom of contract that underlies the contract law of all European countries. In 2011, this “freedom of contract” principle has been explicitly affirmed by the Commission’s expert group on European Contract Law in its feasibility study. Besides the other affirmed principles of “contractual certainty” and “contractual fairness” it serves as a basis for the further harmonisation of contract law.[229] The European Data Protection Directive 95/46/EC explicitly open up the possibility of lawful data transfers on the basis of appropriate contractual clauses (Article 26 (2) European Data Protection Directive 95/46/EC).

According to Article 26 of the European Data Protection Directive 95/46/EC the European Commission is competent to find that specific Standard Contractual Clauses pose an adequate guarantee within the meaning of Article 26 Paragraph 2 in the context of the procedure described in Article 31 (2) 95/46/EC. The Standard Contractual Clauses developed by the Commission are not the only Contractual Clauses that can be recognized as adequate. In Principle, every company or trade association may draw up contracts and hand it in for the Commission’s approval.[230]

6.2.1.1 Objectives and historical development

The first and foremost goal of providing these standard contractual clauses for usage is the warranty of adequate safeguards for the lawful transfer of personal data. Their contractual guarantees of data protection and provisioning of data subject's rights enable legal certainty and compliance with the European Commission's requirements regarding a sufficient level of protection for the data.[231] The European Commission has adopted several sets of Standard Contractual Clauses covering different roles of the data recipient. The recipient can either take the role of a data controller or a data processor. So an important pre-condition of using

[229] Commission Expert Group on European Contract Law, *Feasibility study for a future instrument in European Contract Law*, 3 May 2011

[230] Cf. article 26 (4) EU Data Protection Directive 95/46/EC

[231] See also Article 29 Working Party, WP 74, *Working document: Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers, adopted on 3rd June 2003*, p.7

these clauses is the determination which role the involved parties obtain. This depends on the explicit and implicit competence as well as the factual control of the party. In a nutshell, the amount of decision power over the purpose and means of the data processing determines the classification either as controller or solely as processor.[232] Once the involved parties have been identified either as controller and processor, they need to use the fitting set of standard contractual clauses provided by the European Commission in the correct context. The Commission provides three different sets of clauses currently in force, whose applicability is determined to which parties the data is transferred. There are two different constellations of data transfers:

- Transfer of data from controller to another controller (C2C)
- Transfer of data from controller to a processor (C2P)

Two of the three sets provided by the European Commission cover the C2C constellation. These Commission decisions on these two sets are from the years 2001 and 2004:

- Commission Decision of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC (2001/497/EC)

And the alternative set, amending the first:

- Commission Decision of 27 December 2004, amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries (2004/915/EC)[233]

The two controller-controller sets are alternatively. Companies may choose their preferred contractual clauses.

The third set covers the C2P constellation, decided by the 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 (2010/87/EU). Before May 2010, a former version of clauses was implemented by Commission decision and in force since 2001.[234] This Commission decision however, was repealed and replaced by the 2010/87/EC Decision. So for the controller-processor data transfer there is no possibility to choose from the 2001 or the 2010 clauses. In cases of newly allocated agreements, the involved parties are bound to implement the 2010 version if using the European standard contractual clauses. An exception just may be valid for older contracts concluded before 15th May 2010, as long as the original agreements remain unamended to that date. Any substantial change of the agreement, for instance by involving new parties or changing the purpose of the transfer, leads to the downgrading of the old clauses as ad-hoc contract, that must be brought into line with the principles and safeguards entailed by the newer clauses of the decision 2010/87/EU. Also, such an ad-hoc contract must be examined and authorised by the concerned data protection authorities. Usually, in such cases it would be more appropriate and easier to

[232] Article 29 Working Party, WP 169, *Opinion 1/2010 on the concepts of "controller" and "processor", adopted on 16 February 2010*, p. 10 ff.; for an overview of and introduction to the criteria for role determination, see TClouds report R1.2.1.2 (*Analysis of EU Law*), p. 14 ff.

[233] This set was approved by the Commission as a result of a request by an affiliation of business associations led by the International Chamber of Commerce (ICC)

[234] Commission Decision *of 27 December 2001 on standard contractual clauses for the transfer of personal data to processors established in third countries, under the Directive 95/46/EC (2002/16/EC)*

directly concluding a new contract using the newer standard contractual clauses 2010/87/EU.[235]

6.2.1.2 Regulated content

This section will illustrate the substantive points of the standard contractual clauses sets and their most significant differences and effects compared to each other. One of the most prominent arrangements is the definition of a data exporter and the data importer. The data exporter is the controller entity that transfers the data while the data importer is the entity that receives the data from the controller. In contrast to the exporter, who is always the controller, the importer can be a controller as well as a processor entity. The specific definition of the data importer can be acquired out of the individual standard contractual clause that should be used, depending on the classification of the receiving party as controller or processor.[236] As already introduced in the prior section, two of the three sets currently in force are related to transfers of personal data from a controller to another controller entity (C2C clauses). In contrast, the third set focuses on the data transfer from a controller to a processor and further sub-processing connections (C2P clauses). Thus, the analysis of the clauses will be broken down in two following sections, thematically divided into C2C clauses and C2P clauses.

6.2.1.2.1 C2C clauses 2001/497/EC and 2004/915/EC

The foremost purpose of the EU standard contractual clauses is the creation of an adequate level of protection for the personal data, allowing the disclosure of said data from the controller to another party. This comes with the regulation of obligations for the individual contract parties and corresponding rights for concerned persons, namely the data subjects to enforce these. The breach of contractual obligations with regard to the personal data is explicitly subject to the liability of the data exporter and the data importer. Difficulties arise once several layers of vendors and customers are involved, igniting the need to conclude a multitude of contracts (cf. the simple example shown in figure1 next page). This especially applies if data are transferred in a chain of several sub-processors, because each data exporter needs to conclude a contract with each data importer in a third country. The adjustment of contracts is even more complex in cases of changes regarding the data transfer itself. Also, once units of an internationally operating corporation are involved or the legal structures of the corporate form change, considerable administrative effort has to be made to align, adjust and newly conclude existing contracts. This also affects contractual structures such as master agreements with added appendices, e.g. related to economic aspects, such as Service Level Agreements, sales and distribution, marketing, or pricing.[237] In the standard contractual clauses provided by the Commission, the applicable law will also be regulated, which is especially of importance for companies with an establishment outside the EU, the EEA respectively. This also implies the determination of concerned data protection authorities and the enforcement of civil law claims against group companies in third countries.

---

[235] Article 29 Working Party, WP 176, *FAQs in order to address some issues raised by the entry into force of the EU Commission Decision 2010/87/EU 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, adopted on 12 July 2010*, p. 4 ff.

[236] Cf. definitions section of the individual standard contractual clauses

[237] These may under certain circumstance be valid as long as they do not contradict the standard contractual clauses, see recital (5) of the Commission Decision 2001/497/EC or recital (4) of the Commission Decision 2010/87/EU.

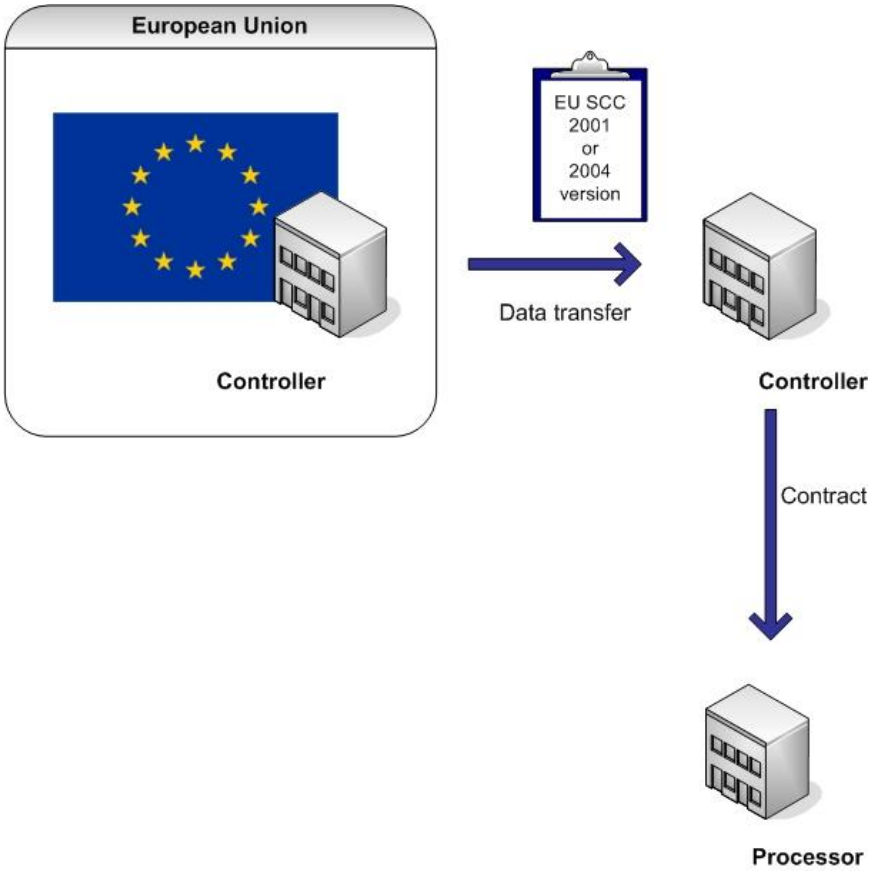


Figure 2: Controller to controller (C2C) constellation

The two sets of clauses 2001/497/EC and 2004/915/EC for the controller-controller data transfer however, show some essential differences. This affects partially some terminology but mostly obligations and liability regulations on both sides of the contract parties. So in the 2001 version (hereinafter: set I), clause 6 (2) provisions joint and several liability of data importer and data exporter, regardless of causation and possibilities of indemnity and compensation agreements. This regulation was replaced by a liability rule following the causation principle under III. (a) of the 2004 version (hereinafter: set II). Also, punitive damages were explicitly excluded. Furthermore, in cases of dispute, the set I provided under 7 (2) an agreement of international commercial arbitration. This solution however, is quite intricate and expensive for the contract parties, thus in most cases not fitting for disputes in the data protection field. Set II does not provide such an arbitration clause. Furthermore, clause 5 (c) of set I requires the contract partners to abide the advice of the concerned supervisory authorities while set II just provisions the accordance with binding decisions (clause II. (h) - (ii)). Beneficial for the contract parties is also the fact that set II opens up the possibility under clause VII. to supplement the contract with commercial clauses and to update the Annex B (under the condition that the concerned authority is informed).

In conclusion to the points elucidated above, set II may appear much more desirable for companies intending to use the EU standard contractual clauses. This also applies for cloud computing contexts, since the complexity of tied services, the potential variety of involved parties and the business philosophy of increased flexibility in regard to data flows, computing and storage capacities require a more flexible coordination and content management of contractual agreements. Thus, set II seems more convenient for cloud computing service providers to use.

6.2.1.2.2 C2P clauses 2010/87/EU and former clauses 2002/16/EC

The new set of clauses based on the Commission Decision 2010/87/EU cover the constellation of data transfers from a controller to a data processor (see figure 2 below). This decision was initiated by a proposal of a number of business associations[238] under the lead of the ICC in 2006[239] because the older version of Decision 2002/16/EC was deemed faulty due to the economic necessity and common practices on the market.

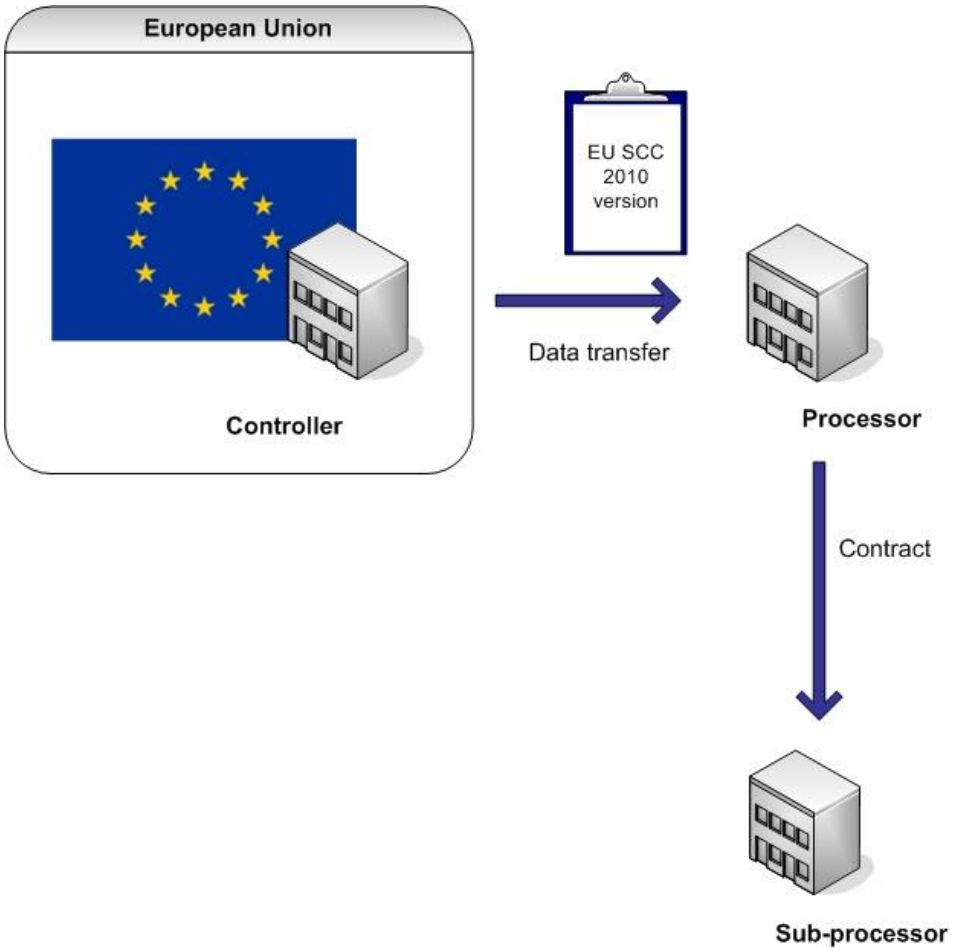


Figure 3: Controller to Processor (C2P) constellation

In response to the proposal by the ICC and its affiliated business associations, the European Commission included some alterations and novelties in comparison to the repealed standard contractual clauses in the 2010 version.

[238] Consisting of the American Chamber of Commerce to the European Union (AMCHAM EU), Japan Business Council in Europe (JBCE) and the Federation of European Direct and Interactive Marketing (FEDMA)

[239] Proposal text of the ICC can be found here:

http://www.iccwbo.org/uploadedFiles/ICC/policy/e-business/pages/BRUSSELS-1257-v1-Controller_to_processor_clauses_submission_October_2006.pdf .

The most significant regulations and changes are:

- Determination of the governing law, being the law of the data exporter's country
- Liability scheme, deploying the data exporter as primarily liable
- Introduction of a sub-processing clause
- Obligation regulations with explicit constraint demands for sub-processors
- Disclosure of contract copies to data subjects and exporters
- DPA powers for auditing and decision authority on agreements with sub-processors under contradicting law
- Deletion of arbitration clause

Clause 9 of the 2010 set of SCC explicitly determines the governing law with regard to data protection aspects as being the one of the member state the data exporter is established in. This rule also applies for sub-processing services through the whole chain of data processing operations. Corresponding to the applicability of the data exporter's national law, the new set of clauses introduces a liability scheme via clause 3 that determines the data exporter, namely the controller, as primarily liable towards the data subject's claims (clause 3 (1)). However, if the data exporter factually disappeared, ceased to exist in law or became insolvent, according to paragraphs (2) and (3), the data subject may follow the chain of contracts and issue his claim against the data importer, which is in this set of clauses and constellation the processor. The same procedure may take place if also the data importer is not assessable for the data subject's claims. In these cases the data subject may even issue his claim against the sub-processor. However, his liability is limited to his own processing operations under the clauses; thereby he may only be held responsible for issues that are within his own factual control. In conclusion, clause 3 (2) and (3) create kind of successor liability to ensure the protection of the data subject through the case-dependent utmost accessibility of a liable party.

The main novelty of the Commission Decision 2010/87/EU is the introduction of a regulation for sub-processing agreements, including a first-time definition of the term "sub-processor". According to clause 1 (d) of the SCC, a sub-processor is

> *"any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract."*

Clause 11 hereinafter introduces the main provisions of the involvement of sub-processors. Such sub-processing agreements from a non-EEA processor to an also non-EEA sub-processor may take place under four explicitly stated preconditions. These will be explained in the following:

- Prior written consent

The data importer that wants to contract with a sub-processor needs to obtain a prior written consent from the data exporter. In such cases, the data importer should communicate his sub-contracting intentions to the data exporter, namely the controller and seek approval thereof.

- Written agreement between data importer (processor) and sub-processor

The agreement between the data importer (processor) and the sub-processor must be in written form.

- Fulfilment of compliance and due diligence requirements

This written agreement between data importer (processor) and sub-processor must be compliant with the instructions of the data exporter (controller). In this context, the data importer is burdened with a due diligence obligation to contractually bind the sub-processor by imposing the same obligations as are imposed onto him under the EU SCC. This also includes obligations after the termination of the contract, such as returning or destruction the personal data after the termination of the processing service (clause 12). The acceptance of the obligations by the sub-processor may optionally be done by co-signing the EU SCC or by another contractual agreement adopting the terms of the controller-processor agreement itself.

- Integration of a third-party beneficiary clause

The written agreement between the data importer and his sub-processor must include a third–party beneficiary clause corresponding to clause 3 of the EU SCC to ensure an unbroken chain of liability to protect the data subject's rights. The sub-processor's liability however, may be limited to his own processing operations, excluding events that are not under his control.

Beyond the sub-processing regulations, the new set of clauses entails some more specific provisions. Just as in the set II of 2004 for C2C constellations, the arbitration clause has been deleted. Another fundamental regulation extracts from clause 5 (f), according to which the data importer is bound to make a copy of the sub-processing agreement available upon request of the data subject. This obligation however, is limited to the extent that he must disclose the contract copy but just a summary of security measures and may exclude commercial information. This procedure may suffice to suitably perform this information duty towards the data subject. Furthermore, clause 5 (j) provisions the sub-contracting must be communicated to the data exporter per default, regardless of a filed request. Clause 11 (4) regulates that the data exporter must keep a list of all sub-processing agreements to be able to eventually provide them to the data protection authority. This list shall be updated once a year. This kind of know-thy-sub-processor procedure entails the data importer sending a full contract copy so the data exporter may be able to fulfil his own obligation to keep track of the closed sub-contracts concerning his transferred data.

By the introduction of the new set of standard contractual clauses via Commission Decision 2010/87/EU, the data protection authorities have been empowered by clause 8 (2) with the authority to conduct audits of all data importers as well as all sub-processors to ensure the compliance of the personal data processing chain with the law of the member state in which exporter is established. Beyond this, the data protection authorities have the power to suspend the transfer of data to such sub-processors if a new legislation in the country of the sub-processor contradicts the provisions of the European data protection law as laid down in Article 4 (1) (a) of the Commission Decision.

Attention should be paid to the non-applicability in cases of a data transfer from an EEA-located data processor to a sub-processor outside the area. However, the fact that the 2010 decision explicitly excludes such constellations may lead to a cumbersome competitive disadvantage for EEA processors who want to contract with a sub-processor outside the EEA. In contrast to non-EEA processors, they are burdened with more administrative efforts

for their sub-processing contracts since they have to align them with their current legal system.[240] Also, recital 23 of commission decision states that

> "*Member States are free whether to take account of the fact that the principles and safeguards of the standard contractual clauses set out in this Decision have been used to subcontract to a sub-processor established in a third country with the intention of providing adequate protection for the rights of data subjects whose personal data are being transferred for sub-processing operations*".

Consequently, the local data protection authorities may be empowered by the individual member states to acknowledge these standard contractual clauses as effective to ensure an adequate level of protection for the personal data in situations when data exporter and processor are located in the EEA and the sub-processor is established outside the EEA. However, it may be possible that in the wake of the revision of the European data protection framework, the European Commission may eventually adopt a new Decision with standard contractual clauses covering the EEA processor to Non-EEA sub-processor constellation.[241]

6.2.1.3 Preconditions for validity

The European Commission stated explicitly in their decisions that the standard contractual clauses may not be altered in any way, especially not by amending the individual sets or merging them.[242] However, it must be taken into account that besides the usage of the European standard contractual clauses the national law of the individual EU member states may require additional regulation. Since the EU SCC should not be changed to avoid risking their legal invalidity, such specifics consequently can only be settled in separate contracts, Service Level Agreements (SLA's) or in an annex to the SCC's, respectively. An example for such specific national requirements derives from Germany, whose law just permits the processing of personal data on behalf of others only under certain preconditions laid down in a ten point's catalogue in Article 11 BSDG (Bundesdatenschutzgesetz).[243] Generally, the allowance of data transfers is examined in a two-step evaluation by the local data protection authorities. First, the general legitimacy of a personal data transfer within the EU or EEA is examined by means of the national data protection law. Once data transfers into a third country outside the community are involved, they must be assessed in terms of permissibility according to section 4c BDSG, which requires the fulfilment of far more stringent provisions. Also, the 2004 set of the EU SCC is seen quite critical by German data protection authorities in regard to the German employee data protection law, because the information obligation of the data exporter is limited. This may lead to gaps in the protection of said data if it is subject to company group-internal data transfers.[244] This issue is also seen critically by the French

---

[240] Article 29 Working Party, WP 161, *Opinion 3/2009 on the Draft Commission Decision on standard contractual clauses for the transfer of personal data to processors established in third countries, under Directive 95/46/EC (data controller to data processor)*, adopted on 5 March 2009, p. 3.

[241] The Article 29 Data Protection Working Party already urged the European Commission to do so by introducing a new legal instrument for such constellations, see footnote 15 above.

[242] Cf. recital (3) of the Commission Decision 2004/915/EC. Also, the amendment of 2001/497/EC by article 1 (1) of the 2004 decision commits the unchangeableness of the clauses. Furthermore, implemented by the Commission Decision 2010/87/EU for C2P constellations, the irrevocable nature of the clauses is stated in clause 10 of the contract text itself (Variation of the contract).

[243] Cf. EuroCloud Deutschland eco e. V. through its Guidelines Cloud Computing German Law, Data Protection & Compliance with advice on contractual regulation to achieve compliance with the German data protection law.

[244] Cf. position paper of the working group "Internationaler Datenverkehr" ("International data transfer") of the German data protection authorities of 28 March 2007, p. 2 section II. 2.

Data Protection Authority (Commission Nationale de l'Informatique et des Libertés, CNIL).[245] It must be noted that this second set is acknowledged by the European Commission as valid also for employee data. Still, it may be advisable to install extra protection mechanisms in favour of the company's (resp. controller's) employees.[246] Other EU member countries may have specific regulations in certain areas as well. So unlike in Germany, in the United Kingdom it is not necessary to undergo a two-step evaluation prior to the data export based on the EU SCC. Still, the UK Information Commissioner's Office (ICO) reserves the right to investigate the contractual agreement of a UK data controller in breach of contract cases.[247] In contrast, in France, the contract clauses regulating the transfer of personal data into third countries need to be reviewed and authorised by the French Data Protection Authority (CNIL). Some few and restrictively handled exceptions are made in cases of prior explicit consent of the data subject or indispensable necessity of the data transfer to safeguard the individual's life or the public interest.[248]

6.2.2 Codes of Conduct

Codes of Conduct are a collection of guidelines and rules for behaviour and ethics. Code of Conduct is the general term describing any kind of unilateral self-commitment of a company to a common set of principles.

Codes of Conduct may be applied in several different sectors and environments. Due to its freedom in regard to content and shape and level of detail, it is able to cover a wide range of subjects. Codes of Conduct proved to be a sufficient approach to regulate in-house policies concerning e.g. combating corruption, service quality or working hours.

In some branches the implementation of similar Codes are regarded as best practice and not implementing them is a competitive disadvantage.

In contrast to Standard Contractual Clauses the Code of Conduct is a unilateral declaration. Therefore, its liability bases on the voluntary commitment of the company. Only if the company wants to be liable for breaches of the Code of Conduct, it has to install measures for internal or external binding penalties. Critical issues here arise from the lack of legally binding effect for the concerned company if it has not installed any voluntary penalty mechanisms. An example of a code of conduct for CSPs is the "Code of Practice" of the Cloud Industry Organisation Limited (CIF). The CIF developed its code of conduct to certify cloud providers in the UK.

The CIF is a non-profit company that is held by several cloud providers. The company was founded in 2009 and its scope is limited to cloud providers in the UK or third parties operating data centers that reside in the UK.[249] The CIF's goal is to help customers to evaluate the different cloud providers according to a common standard. This standard is the possibility for cloud providers to enact the "Code of Practice" which can then be certified by the CIF. The certification process approves the formal compliance of a CSP's Code of Practice to the

[245] Laurence Dumure Lambert and Régine Goury in Meyer Brown L.L.P., *New EU Standard Contractual Clauses for Commissioned Data Processing*, publication of September 2010, p. 8.

[246] This is recommended by the ad-hoc working group "Konzerninterner Datenverkehr" (Intra-group data transfer) in its working report of 11 January 2005, which was constituted by initiative of the Duesseldorfer Kreis, an association of the German supreme supervisory authorities for data protection in the non-public sector.

[247] Mark A. Prinsley and Oliver Yaros in Meyer Brown L.L.P., *New EU Standard Contractual Clauses for Commissioned Data Processing*, publication of September 2010, p. 7.

[248] Ibid., footnote 13.

[249] http://www.cloudindustryforum.org/cif-public-declaration .

standards set up by the CIF. After paying the registration fee, the self-certification process must be satisfactorily shown to the CIF. A CSP's Code of Practice must include statements about Transparency, Capability and Accountability of the CSP.[250] Despite being a self-commitment that is only formally verified, the CIF reserves the right to conduct audits of the claims made. In case a CSP does not comply fully with the code, the CIF withdraws the certificate and imposes a monetary penalty.[251]

CSPs can decide to become either active or passive members of the CIF. As those, they can either actively participate in the creation process of the certification requirements of the Code of Practice or passively vote on them, respectively. However, there is no restriction that a certified CSP cannot be a member that actively forms the Codes of Practice.

Specific legally binding Codes of Conduct in regard to privacy are Binding Corporate Rules.

6.2.3 Binding Corporate Rules

Besides a contractual agreement between involved parties, an alternative instrument to undertake the regulation of data protection, are the so-called Binding Corporate Rules (BCR).

6.2.3.1 Nature and Scope of Application

BCR are corporate codes of conduct that legally bind each entity of a conglomerate to company-specific, EU-compliant data handling systems. Under BCR, a multinational group develops its own in-house regulatory structure sheltering the data processing of its branches and units worldwide. Once approved, BCR empower the multinational group to transfer personal data of EU data subjects in-house, worldwide.

In WP 74, the Article 29 Data Protection Working Party states for the first time that BCR could be a suitable basis for cross-border data transfer. [252]

The term "binding corporate rules for international data transfer" was suggested by the Article 29 Data Protection Working Party (WP 29) as appropriate, because it reflects adequately the purpose of their existence.

- "Binding Rules" indicates that in order for these rules to be deemed as "sufficient safeguards" within the meaning of Article 26 (2) 95/46/EC, they must have internal and external binding effect
- "Corporate" refers to the context in which these rules can be applied; a multinational group drafts and implements these rules, usually under the responsibility of the headquarters.
- "International data transfer" reflects the reason for the application of this code of conduct; it provides a legal basis for cross border data transfers within a multinational group.

An alternative proposal was the more unwieldy term "legally enforceable corporate rules for international data transfer". As of 2005 the Article 29 Data Protection Working Party abbreviated the term to "Binding Corporate Rules".[253] The instrument BCR does only concern

[250] http://www.cloudindustryforum.org/downloads/ip10-the-code-of-practice-v6.1.pdf .

[251] http://www.cloudindustryforum.org/downloads/ip10-the-code-of-practice-v6.1.pdf .

[252] Article 29 Working Party, WP 74 pp. 6-7.

[253] See Article 29 Working Party, WP 107.

transfers within a multinational group.[254] Transfers of personal data outside of this group are not governed and therefore not legitimised by BCR. Hence, these onward transfers of personal data of European data subjects have to be on the basis of other "legitimate grounds" under Article 26, 95/46/EC (e.g. SCC or individual contractual solution approved by the concerned DPA).[255]

„BCR are a kind of group-wide company privacy policy that must fulfil a couple of requirements set forth by the European Commission. The BCR must be shown to have legally binding effect both internally between the group companies, employees and subcontractors and externally for the benefit of individuals. All companies belonging to the group are then considered to ensure an adequate level of data protection. Accordingly, BCR only apply to intra-group data transfers, but not to transfers to entities outside the group. Also, despite of some simplifications in the close past, the implementation of BCR is still a time consuming task causing considerable administrative burden." [256]

6.2.3.2 Process of Approval

WP 107 and 108 set forth a general procedure under which multinational enterprise groups that export data from several EU member states may seek approval of all concerned national data protection authorities.

6.2.3.2.1 Selection of the Lead DPA

The initial step is to select a lead DPA. The group making application has to choose the lead DPA based on five criteria:[257]

- Location of the group's European headquarters
- Location of the group's unit responsible for data protection
- Location of the group's unit that is most appropriate for dealing with the application and enforcement of BSR within the group
- Place where most decisions regarding purposes and means of data processing are taken
- EU member states from which most transfers outside the EEA will take place

The applicant will approach the DPA it considers as the designate lead ("entry point"). It should provide the entry point with all information regarding the general structure of the group and its data processing activities in the EU/EEA (especially the locations where decisions are made, the location and nature of EU affiliates, the number of persons concerned, the places from which export from the EU takes place) and the countries to which those data are transferred.[258] The DPA receiving the application "will exercise its discretion in deciding whether it is in fact the most appropriate".[259] The entry point then forwards information regarding the decision on the lead DPA to all other concerned DPAs with the indication of whether or not it agrees to be the lead DPA.

---

[254] Article 29 Working Party, WP 74 p. 9.

[255] Article 29 Working Party, WP 74 p. 9.

[256] Helbing, *How the New EU Rules on Data Export Affect Companies in and Outside the EU*, 2010.

[257] Article 29 Working Party, WP 107 p. 2.

[258] Article 29 Working Party, WP 107 p. 3, see also WP 108 pp. 3-4.

[259] Article 29 Working Party, WP 107 p. 2.

If the entry point considers itself the appropriate lead DPA, the other DPAs are asked to raise objections within two weeks.[260] The period is extendable up to additional two weeks if requested. If the entry point does not agree to be the lead DPA, it should give its reasons and recommend a lead DPA, in which case the affected DPAs shall endeavour to decide the matter within one month.

6.2.3.2.2 Approval of BCR

Once the decision on the lead DPA has been made, the latter starts negotiations with the applicant. As a result of these negotiations, the lead DPA will circulate a "consolidated draft" of the BCR to all concerned DPAs, who may comment within one month.[261] After this period, the lead DPA will communicate these comments to the applicant and resumes negotiations, if necessary.[262] Together with the lead DPA the applicant will address the comments and elaborate a "final draft", which has to be confirmed by all concerned DPAs.[263]

This confirmation is regarded as an agreement "to provide the necessary permit or authorisation at national level".[264] Additional requirements on national level such as notification or administrative formalities remain unaffected.[265]

After the approval the Chairman of the Article 29 Data Protection Working Party has to be informed and will share this information with other EU/EEA's DPAs immediately.[266]

The consolidated draft should be provided in the leading DPA's language and English. The final draft should be translated into the languages of all involved DPAs.[267]

6.2.3.2.3 Mutual Recognition

Although the Documents of the Article 29 Data Protection Working Party are not binding for the national DPAs, most of them support this cooperation procedure.[268] Nevertheless, this procedure was often criticised for being too time consuming and imponderable, as it "allows the DPAs to request country-specific additions, exercise de facto vetos or even refuse to participate".[269]

To support and accelerate the cooperation several national DPAs have agreed upon a mutual recognition. If the lead DPA acknowledges that the BCR are a adequate safeguard for personal data, the other participating DPAs have confidence in this decision and accept the findings of the lead DPA under this mutual recognition agreement As of April 2011, the 19 countries taking part in mutual recognition are as follows:[270]

---

[260] Article 29 Working Party, WP 107 p. 3.

[261] Article 29 Working Party, WP 107 p. 3.

[262] Article 29 Working Party, WP 107 p. 3.

[263] Article 29 Working Party, WP 107 p. 3.

[264] Article 29 Working Party, WP 107 p. 4.

[265] Article 29 Working Party, WP 107 p. 4.

[266] Article 29 Working Party, WP 107 p. 4.

[267] Article 29 Working Party, WP 107 p. 4.

[268] Mesaikou, *Examining the Binding Corporate Rules as the most promising solution for the cross border data transfers of multinational companies under the EU Data Protection Directive*, p. 22.

[269] Mesaikou p. 22.

[270] ICO
http://www.ico.gov.uk/for_organisations/data_protection/overseas/binding_corporate_rules.aspx

- Austria
- Belgium
- Bulgaria
- Cyprus
- Czech Republic
- France
- Iceland
- Ireland
- Italy
- Latvia
- Liechtenstein
- Luxembourg
- Germany (Federal and Länder)
- Malta
- Netherlands
- Norway
- Slovenia
- Spain
- United Kingdom

This agreement does not represent a formal change to the established procedure or an impairment of the legal sovereignty of the national DPAs. The mutual recognition is more of a policy commitment, based on trust and the presumption that the Data Protection Directive guarantees an equal standard of privacy and data protection in all European member states.[271]

6.2.3.3 Necessary Content

BCR are a tailor made solution for one multinational group. Therefore, the content of BCR differs depending on different conditions and needs of each conglomerate. Further implications on the variety of possible contents have the types of data processed as well as the legal requirements and characteristics of the countries where the data transfer takes place.[272] The Article 29 Data Protection Working Party has adopted a number of Working Papers adumbrating the substantial content of BCR[273] to facilitate the drafting of BCR for the applicants.

[271] Mesaikou p. 22.

[272] Mesaikou p. 16.

[273] Article 29 Working Party, WP 108, 2005; WP 133, 2007; WP 153, 2008; WP 154, 2008; WP 155, 2008.

6.2.3.3.1 Legal Enforceability

BCRs have to ensure, that they are legally enforceable. They should declare to be binding, externally for the benefit of individuals as well as within the multinational group and even within a single unit of the group.[274]

6.2.3.3.1.1 Internal Enforceability

The Article 29 Data Protection Working Party suggests different mechanisms to safeguard the internally binding character for the members of the multinational group:[275]

- Binding corporate or contractual rules that one can enforce against the other members of the group
- Unilateral declarations or undertakings made or given by the headquarters or parent company, which are binding on the other members of the group
- Incorporation of other regulatory measures, e.g. obligations contained in statutory codes within a defined legal framework
- Incorporation of the rules within the general business principles or corporate governance codes of the group backed by appropriate policies, audits and sanctions

The last suggestion is indeed recommended as it turns BCR into a "sub-policy" of the group and hence already existing compliance mechanisms in place, e.g. internal audit systems, can also apply to privacy and data protection as outlined in the BCR.[276] These suggestions may have a different effect in different EU member states. For example, simple unilateral declarations are not regarded as binding in some member states.[277] The applicant should therefore consult local DPAs if it intends to rely on a unilateral declaration.

Also, the Rules have to be internally binding for the employees of the group. The Article 29 Data Protection Working Party suggests to incorporate specific obligations in a "contract of employment" and by enforcing these obligations by disciplinary procedures.[278] Additionally, the compliance should be safeguarded by adequate training programmes and senior staff commitment.[279]

Last but not least the applicant has to prove that his subcontractors are bound by the BCR. He hast to provide evidence to the lead DPA of the contractual clauses that are imposed on subcontractors and explain the consequences of non-compliance of a subcontractor.[280]

6.2.3.3.1.2 External Enforceability

BCR have to be externally binding as well. Data subjects should be awarded with third party beneficiary rights. This means, individuals covered by the scope of the BCR must be able to enforce compliance "both via data protection authorities and the courts".[281]

---

[274] Mesaikou p. 18.

[275] Article 29 Working Party, WP 108 p. 5.

[276] Mesaikou p. 19.

[277] Article 29 Working Party, WP 108 p. 5.

[278] Article 29 Working Party, WP 108 p. 5.

[279] Article 29 Working Party, WP 108 p. 5.

[280] Article 29 Working Party, WP 108 p. 6.

[281] Article 29 Working Party, WP 108 p. 6.

If under the legal system of a member state these beneficiary rights cannot be granted by unilateral declarations, the group should put in place corresponding contractual agreements.[282]

The BCR have to include an agreement conferring jurisdiction. Individuals must be able to commence claims within the jurisdiction of the member of the group at the origin of the transfer or the EU headquarters or the European member of the group with delegated data protection responsibilities.[283]

To ensure efficient rights of the data subject, the BCR have to be made publically available. The data subject must get informed about the responsible contact for addressing complaints and the complaint handling process.

Ultimately, the group has to provide sufficient assets or provides appropriate arrangements to enable payment of compensation for any damages resulting from the breach of the BCR.[284]

6.2.3.3.2 Verification of Compliance

WP 74 states that the binding corporate rules adopted by an organisation must provide for the use of either internal auditors, external auditors or a combination of both. The audit programme should adequately cover all aspects of the BCR and allow the competent DPA to carry out data protection audits if required.[285]

6.2.3.3.3 Identification of Data Processing and Data Flows

The BCR should identify the categories of data that are transferred (e.g., customer data, human resources) with sufficient detail to enable the competent DPA to determine whether adequate safeguards against e.g. unauthorized use and disclosure are in place. The BCR should also describe the purposes for which the data are collected and processed.[286]

In addition, the applicant has to define the scope of transfers that are covered by the BCR, whether they cover only transfers from the EU or whether all transfers between members of the group are covered, which includes intra-EU transfers. The concerned DPAs furthermore have to be informed on what basis onward transfers (e.g. transfers of data from group members outside the EEA to third parties) take place.[287]

6.2.3.3.4 Data Protection

The BCR must also contain a clear description of the data protection safeguards consistent with Directive 95/46/EC and must set out how they are met within the group. In particular, they have to address transparency and fairness to data subjects, purpose limitation, ensuring data quality, security, individual rights of access, rectification and objection to processing and restrictions on onward transfer outside of the multinational group.[288]

[282] Article 29 Working Party, WP 74 p 11.

[283] Article 29 Working Party, WP 108 p. 6.

[284] Article 29 Working Party, WP 108 p. 6.

[285] Article 29 Working Party, WP 108 p. 7.

[286] Article 29 Working Party, WP 108 p. 7-8.

[287] Article 29 Working Party, WP 108 p. 7-8.

[288] Article 29 Working Party, WP 108 p. 8.

6.2.3.4 Drawbacks and Benefits

Though corporate groups seemed reluctant to implementing BCR in the beginning, they became more and more popular in recent years. Several companies applied for BCR in cooperation with different lead DPAs all across Europe. Some examples of companies that have implemented sufficient BCR are the Atmel Corporation (for human resources data) as of April 22nd 2009, Accenture Limited (for human resources and customer data) as of April 30th 2009 and the Hyatt Hotel Corporation (for human resources and customer data) as of September 9th 2009. Each corporate group has to weigh the advantages and disadvantages to examine if BCR are appropriate for its needs.

6.2.3.4.1 Drawbacks

BCR "are not for the fainthearted or the tight-budgeted".[289] Despite its humorous twist, this apt quotation picks up on two main drawbacks regarding BCR. Regulations covering several branches of a multinational group and data flows crossing national borders prove to be very complex. The creation and implementation consume lots of time and money.

One further problem is the imponderability of the approval. Though many national DPAs have agreed upon the mutual recognition policy, some DPAs seem unwilling to waive their power over regulatory matters for a foreign lead DPA.[290] Under the procedure laid out in WP 107 each concerned DPA can demand changes to the draft BCR, which might result in a lengthy and costly approval period.

Moreover, the legal implications of BCR are still uncertain. The national DPAs do not have an understanding regarding the legal effect of BCR. While the Netherlands regard the group as a "Safe Harbour" which permits data transfer without an additional approval by the DPA, many other DPAs, e.g. France and Germany, still demand approval for the data transfer on basis of the BCR.[291] "However, in this case they argue that in order to give their approval they will check the compliance of the data transfer with the requirements set up in the BCRs themselves an not in the local data protection laws."[292]

Additionally, for loose conglomerates, BCR are unlikely to be a suitable tool for international data transfer. The diversity between the units and the broad scope of processing activities make it difficult to impossible to implement and enforce adequate BCR. "For these conglomerates it would be necessary to differentiate subgroups within the same corporate group, set up severe limitations and conditions for the exchanges of information and particularise the rules."[293]

Multinational groups might find another disadvantage in the fact that it is required to implement a process for internal (by independent auditors) and external audits (by the DPA). WP 153 grants the DPA the right to examine the reports of the internal audits. This cooperation with the national DPAs might oppose the group's confidentiality.

The last major drawback of BCR is that this instrument does only concern transfers within a multinational group. Transfers of personal data outside of this group are not governed and therefore not legitimised by BCR and demand for additional contractual measures.

[289] Dowling, *International Data Protection and Privacy Law*, p. 18.

[290] Mesaikou p. 25.

[291] Mesaikou p. 26.

[292] Mesaikou p. 26.

[293] Article 29 Working Party, WP 74 p. 9.

6.2.3.4.2 Benefits

The main advantage of BCR is that they are a tailor-made solution, drafted by the applicant and adjusted to its own special needs. The group has the opportunity to find individual answers to specific issues arising from its own fields of data processing and data flows. Moreover, no other contractual solution provides a similar holistic approach on data protection within one multinational group with several units. With several European data exporting units and several recipients overseas the number of contracts, needed to justify these transfers, multiplies. And each one of this multiple contracts has to be approved by the competent national DPA. In contrast, after the implementation of BCR, the group's members may transfer data without additional contractual safeguards. The group has its own global privacy policy. A privacy and data protection standard is guaranteed even in jurisdictions without any privacy regulations.

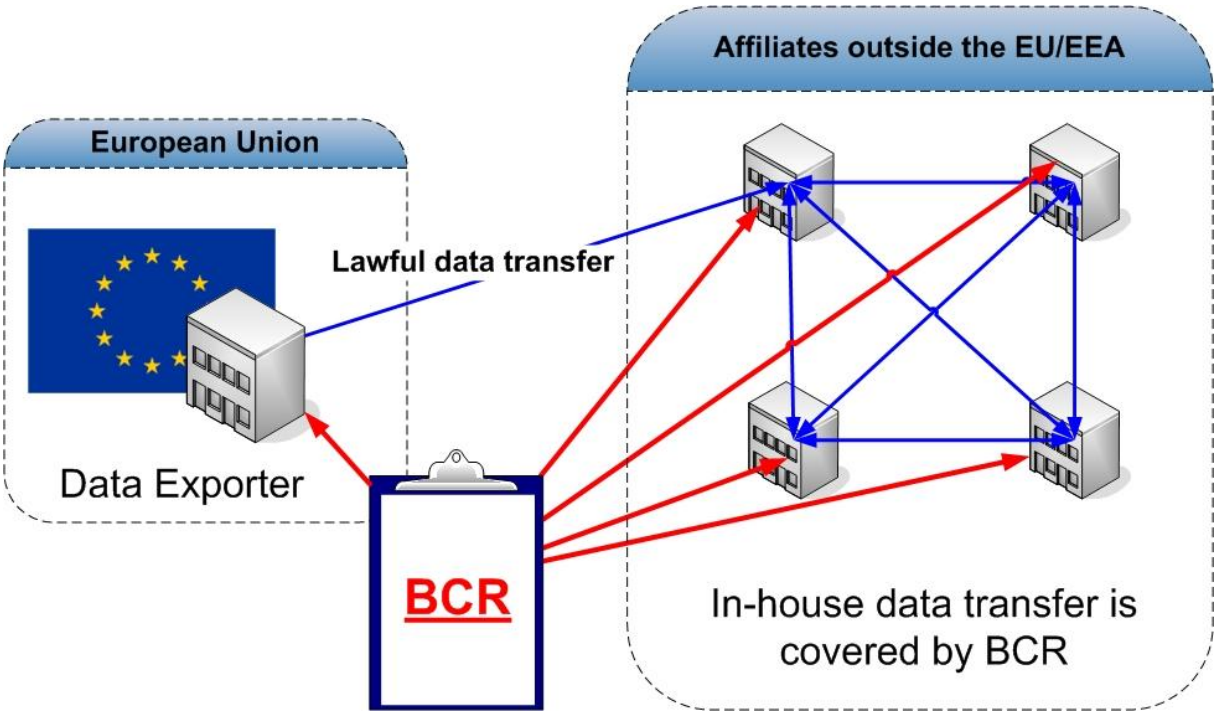


Figure 4 In-house data transfer covered by BCR

BCR are also beneficial for data subjects. They benefit as well from the group-wide identical privacy standards. In case of a infringement, they may contact their local office in their own language. They are furthermore allowed to take legal action at the court designated for the data exporter in Europe.

6.2.4 Contractual and other regulations: Conclusion

The aforementioned bilateral and unilateral solutions to subject the issues around cloud computing to a reasonable and data protection law compliant regulation are surely useful tools to achieve these goals. They are however, not generic and all-embracing instruments for all thinkable constellations. Each of them must be assessed and examined for suitability in the factual situation and tailored to the specific risks of the case. The European Standard Contractual Clauses have been enhanced and improved over the last years but precondition their usage unaltered for their validity. Thus, they lack the flexibility that may be needed to suit either complex operational structures or fast-pacing and constantly changing conditions of personal data processing. Insofar, they are too abstract and non-proprietary to fit exactly

to the specific problem fields regarding cloud computing. Also problematic may prove the lack of harmonisation in regard to the approval procedures with the concerned DPA' s in the different EU member countries. Moreover, there may be restrictions for the implementation in respect to certain categories of data, such as employee data, so complementary protection mechanisms may be needed. At first sight, BCR as a data protection specific kind of Code of Conduct might seem to be a preferable solution for big internationally operating CSP's. They enable cross-border data transfer without further administrative effort, which certainly is beneficial for the flexible and scalable model of cloud computing. But BCR are designed as an in-house solution for one single multinational company. Therefore, CSPs with several (foreign) non-affiliated subcontractors do not benefit, so they still need additional contractual solutions with every subcontractor to allow any onward data transfer. Moreover, for the TClouds approach of a cloud-of-clouds, BCR do not pose a sufficient framework because they do not cover cooperation of several independent CSPs. Thilo Weichert from ULD, the northernmost DPA of the German Länder, suggested that BCR might be adapted to cover non-affiliated sub-processors. But this approach to BCR is not yet officially approved by the Article 29 Data Protection Working Party. Its application and use for transfers to sub-processors and other third parties remains to be seen.[294] Consequently, all these both possible solutions have advantages, but also major drawbacks for CSPs. Within the cloud computing context, EU SCC as well as BCR both need additional measures which nullify their benefits compared to individual contractual solutions in regard to costs and effort.

6.2.5 Audits and certifications as decision support

The customer-sided test of data protection compliance comes with significant hurdles of operational insight and control. The supervision of the data processing at huge server farms and data centres all around the world almost always confronts the user of services with the problem of factual impossibility mostly due to monetary and organisational restrictions. Also, the service providers desire to protect their business by hindering an all-embracing insight to their internal affairs. Therefore, the contractual assignment of audit rights offers a way forward towards the realisation of the required compliance. Advanced and tailored risk assessments, audits and certifications may give the opportunity to establish trust into new cloud computing offers.[295] Also, guidelines for potential customers of services, such as provided by the OECD and ENISA[296], may be helpful to ascertain the security and privacy measures of the providers and achieve the compliance with European data protection requirements. Also, governmental efforts to provide trustworthy and verifiable do exist as well

[294] Wybitul, Patzak, Zeppenfeld, 2010.

[295] First steps into this direction have already been made throughout the cloud industry, for instance by the EuroCloud SaaS Star Audit, developed by EuroCloud Deutschland eco e.V.; cf. also J. Oriol Fit´o and Jordi Guitart, Barcelona Supercomputing Center and Technical University of Catalonia, Barcelona, Spain, *Introducing Risk Management into Cloud Computing*; the effectiveness and trust evolving from instruments offered on the free market will be significantly dependant on the extent of the examination process and the transparency of the criteria used. The future will tell whether the vendors of instruments are able to meet the legal data protection requirements in a suitable way and thereby earn the trustworthiness to provide eligible assurance for potential service customers.

[296] See the OECD *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* and the ENISA document *Cloud Computing - Benefits, Risks and Recommendations for Information Security*, including a useful risk assessment checklist on pages 71-82; see also the decision of the Danish Data Protection Agency in Copenhagen in: *Regarding processing of confidential and sensitive personal data in connection with use of Google Apps online office suit* of 3 February 2011, p. 3, whereas the agency explicitly recommends the usage of ENISA's checklist to ensure the adequacy of a cloud computing risk assessment.

and become increasingly important to meet the requirements of modern time's challenges to data protection and privacy.[297] This applies to cloud computing contexts as well.

6.3 Technical

This section addresses some technical approaches to the critical issues of cloud computing in regard to European data protection requirements.

6.3.1 Standardisation efforts and regulations

Another method of resolution is the encouragement of standardisation efforts and unifying regulations. The EU Data Protection Directive 95/46/EC relates in its Article 17 (1) to appropriate technical and organisational measures to protect the personal data against unwanted incidents. Standardisation and regulation can facilitate the installation of such technical and organisational measures and lead to a significantly wider acceptance and trust into cloud computing services. Furthermore, they may help to enforce a minimum level of security and data protection across the spheres of different service vendors. Efforts in this sense are technical standards like ISO, ITIL, SAS70II and ISAE.

Furthermore, the OECD published guidelines on the protection of privacy and transborder flows of personal data provide some useful information about ideal preconditions for lawful data processing.[298] Thus, they serve as a widely acknowledged international consensus in respect to the collection, storage and processing of personal data. The guidelines laid down core principles that can help governments, companies and service customers to ensure the compliance with the legal data protection requirements to prevent extensive and unlawful data transmissions across borders. Generally, it would be desirable to foster the further development and improvement of such standards and guidelines to empower service providers as well as the customers with suitable tools to realise data protection compliance.

6.3.2 Supporting research and development

Research and development can also provide new approaches to the critical issues comprised in cloud computing contexts. The European Union fosters several research and standardisation projects related to cloud computing funded by the European Commission. Although not all of these projects are solely focused on data protection issues, some of them address organisational and security issues that also may become relevant in respect to European data protection requirements.[299] Also, research in the business world also aims at

[297] Cf. the EuroPriSe European Privacy Seal that certifies IT products and services compliant to the European data protection and privacy requirements on European and national level as well. This European trust mark is an initiative of the data protection authority Unabhaengiges Landeszentrum fuer Datenschutz Schleswig-Holstein (ULD), Germany as a follow-up continuation of a European project funded by the European Commission under its eTEN programme. https://www.european-privacy-seal.eu/

[298] OECD *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*

[299] Prominent examples for cloud computing related projects are: RESERVOIR (http://www.reservoir-fp7.eu/), VISION Cloud (http://www.visioncloud.eu/), OPTIMIS (http://www.optimis-project.eu/) or CONTRAIL (http://contrail-project.eu/).

more advanced service-oriented architectures (SOA's) enhancing privacy.[300] Generally, all-embracing architecture models like the idea of an Intercloud[301] can form the scope of such research as well as individual services providing punctual improvements for single issues, like data minimisation via de-duplication.[302] Also, the extension beyond conventional logging solutions is a focal point of some approaches.[303]

6.3.3 Privacy by Design

A very effective way to encounter the data protection issues in cloud computing is the so-called Privacy by Design (PbD) approach. This concept was first developed by the Canadian Information & Privacy Commissioner Dr. Ann Cavoukian in the 90's and proposes that a company's business processes, namely its offered services and the whole infrastructure around them as well as its related IT systems should be designed privacy-friendly from the very beginning. Privacy by Design encompasses a set of fundamental principles, which are as follows:

- Enabling privacy should be proactive, not reactive; measures should be preventative not remedial
- Privacy should be implemented as the default setting
- Privacy should be embedded into the design of the service/product from the very beginning
- Accommodation of all legitimate interests and objectives by offering full functionality (positive-sum, not zero-sum)
- End-to-end security — full lifecycle protection of personal data from moment of collection to deletion after use
- Visibility and transparency should keep component parts and operations open to independent verification
- Respect for user privacy by offering knowledge and control[304]

---

[300] Liang-Jie Zhang and Qun Zhou, Introduction to Cloud Computing Open Architectures as a new model of SOA's: *CCOA: Cloud Computing Open Architecture*, published for 2009 IEEE International Conference on Web Services

[301] Cf. Todd Hoff, *Intercloud: How will we scale across multiple clouds?*, 5 April 2010; another approach is pursued by Gunnar Peterson, *Don't Trust. And Verify – A Security Architecture Stack for the Cloud*, co-published by the IEEE Computer and reliability societies, issue September/October 2010

[302] Danny Harnik, Benny Pinkas, Alexandra Shulman-Peleg, *Side Channels in Cloud Services - Deduplication in Cloud Storage*, co-published by the IEEE Computer and reliability societies, issue November/December 2010, p 40 ff.

[303] Ph.D. Anton Chuvakin, *Observe PCI DSS: How to Audit Application Activity - When Logs Don't Help*, 2011. In this paper, the author focuses on the insufficiency of the conventional Payment Card Industry Data Security Standard (PCI DSS) in many cases with payment card involvement because of handling difficulties. He explicitly proposes a new approach to the PCI DSS for cloud computing scenarios.

[304] Ann Cavoukian, Ph.D., *Information & Privacy Commissioner Ontario, Canada, Privacy by Design - The 7 Foundational Principles*, originally published: August 2009, revised January 2011, http://www.privacybydesign.ca .

The National IT and Telecom Agency Copenhagen, Denmark, introduce an alternate approach to achieve PbD by Security-by-Design (SbD). IT services must be designed with an architecture that focuses on minimal data disclosure only and always under the control of the user. Also, the relation to an identified or identifiable individual should be hindered by using attribute-based credentials, virtual identities and transaction isolation. These also shall apply to cloud computing contexts, since specifically in such cases there is an increasing need of a trustworthy infrastructure.[305] Cloud computing nowadays is challenged with requirements of availability, integrity and protection of data. Furthermore, it must meet the requirements of regulatory and audit of enterprises.[306] Realisation possibilities could be encryption techniques, comprehensive authorisation/access concepts and correlating access controls, including secure credentials and also logging functions for auditing/forensics. However, the key to lawful business success must be the dispensation of minimal solutions and the orientation towards higher data protection standards.[307]

A study by the consulting firm London Economics on the economic benefits of privacy-enhancing technologies (PETs) for the European Commission revealed that the costs and benefits of PETs vary significantly across technologies. Nevertheless, in those branches, where a demand for such PETs does exist, the relevant service providers may still gain a competitive advantage through an integration into their own products. As for the cloud computing business, such demand for privacy-enhancing technologies definitely exists due to the significant loss of direct control over the personal data by the customer of the service.[308]

6.4 Cloud Computing – Methods of resolution: Conclusion

The previously analysed methods of resolution in regard to the critical issues evolving in a cloud computing context are supposed to encounter difficult sector-specific problems like jurisdiction, outsourced control and the common lack of transparency due to the remote processing of personal data. These problems are even aggravated once cross-border data transmission is involved. Identifying the involved parties in the individual context is essential to enable an appropriate allocation of obligations and legal responsibilities in respect to the protection of personal data in line with the EU Data Protection Directive 95/46/EC. Moreover, deficiencies concerning the enforcement of such legal responsibilities must be addressed both on legislative well as on contractual or company-internal level. Such contractual and other regulations are at any rate helpful tools, equipped with advantages and disadvantages, depending on the individual case. To determine their suitability in the factual situations in question, these advantages and disadvantages need to be analysed and assessed carefully and with utmost effort to achieve satisfying compliance with the use-case specific data protection requirements. Beyond these tools, audits and certifications are no universal remedies due to being a tool still being in its infancy in respect to data protection and cloud

[305] The National IT and Telecom Agency Copenhagen, Denmark: *New Digital Security Models - Discussion Paper*, February 2011, p. 11 ff.

[306] NEC Company, Ltd. and Dr. Ann Cavoukian (Information and Privacy Commissioner, Ontario, Canada) *Modelling Cloud Computing Architecture Without Compromising Privacy: A Privacy by Design Approach*, May 2010, p. 10; also see Ann Cavoukian, *Privacy in the clouds. A white paper on privacy and digital identity: Implications for the internet*, p 25 ff.

[307] Cf. Ann Cavoukian, Ph.D., Martin E. Abrams and Scott Taylor, Privacy by Design: Essential for Organizational Accountability and Strong Business Practices, p. 8 ff.

[308] London Economics, *Study on the economic benefits of privacy-enhancing technologies (PETs*), Final Report to The European Commission DG Justice, Freedom and Security, July 2010, p. 153 ff.

computing issues. Still, they may be helpful to some extent to help with the choice of a potential cloud service vendor that provides services reconcilable with the European and national data protection law. Technical solutions that address the difficulties resulting of cloud computing technologies are definitely promising. This especially applies to the Privacy by Design concept and standardisation efforts. It is certainly desirable to further develop these basic approaches and merge them into the technologies that gain growing importance in the modern every day life of European citizens.

Chapter 7

Cloud Computing: Legal Analysis Conclusion

Privacy and the protection of personal data are the key issues in an increasingly technological world today. The growing use of Internet services, such as webmail, online applications, storage and computing power services, entail a compelling inducement to extensively outsource personal data to foreign servers beyond direct possibility of control or influence. As we have shown with this document, the frameworks of European data protection law, especially the EU Data Protection Directive 95/46/EC apply to cloud computing contexts. Thereby the virtualised processing of personal data in a cloud computing system provides extraordinary difficulties in regard to privacy and data protection. The lack of consumer knowledge about provider-internal business processes and the measures taken to protect the data against security and privacy risks raise severe concerns. Also, legal issues, especially in cross-border data transfer cases are noteworthy barriers to overcome for an ideal exploitation of the cloud computing business model. The current data protection framework, on national level as well as on European level, is often considered as insufficient to meet the technological specifics and needs that arise by the deployment of cloud services. This framework however, already gives us tangible basic conditions for a sensible and lawful processing of personal data that are absolutely applicable to cloud computing solutions. These conditions tackle critical issues like control over data (e.g. the data subject's rights) as well as the transparency on provider side (e.g. notification obligations). Such critical factors need to be overcome with tailored solutions fit for the real individual use cases, may they be of contractual kind (e.g. by EU Standard Contractual Clauses), or through an adaption of data protection requirements by service vendors (e.g. by Binding Corporate Rules or approaches of technical and organisational nature). It will be the challenge of the future to address these issues, to research and develop new solutions that enable a higher level of protection and the compliance with the current legislation. Within this process, the TClouds project aims at making the processing of personal data within a cloud compatible with the European data protection law. The TClouds consortium will make a great part of its results accessible to the public to achieve a greater distribution of privacy supporting approaches in the cloud computing field. To achieve this goal, we pursue a dual approach: technical and legal. A main focus of the technical research will be the design of a trustworthy, federated and secure cloud-of-clouds architecture. This architecture shall provide the grounds of a jointly provision and management of several cloud components and systems with a diversity of services while still maintaining a sufficient level of security and privacy. Also, the development of new open standards is a major concern during this project. From the legal point of view, we will analyse the legal requirements tailored to the project specific use cases of the energy sector and the healthcare sector. These will be addressed in our future reports R1.2.2.1 (Specific legal analysis and requirements: "Smart Lighting") and R1.2.2.2 (Specific legal analysis and requirements: "Patient Monitoring"). With all this work, we will make our contribution to the further advancement of data protection compliant cloud computing technologies and deployment models nowadays.

Chapter 8

Exemplary role model (Annex A)

8.1 Introduction

Current state-of-the-art cloud computing technologies makes it possible for users to access IT-infrastructures of the most diverse kind as flexible and scalable pay-as-you-go services via networks, such as the internet. This involves the utilization of software applications as well as hardware services from different providers. Thus, cloud computing is utmost attractive not only to the public but also to enterprises and municipalities to achieve a considerable reduction of material and human resources expenses. But present-day cloud computing systems comprise severe risks, especially regarding security and privacy. The cross-border collection, processing and storing of data within and outside the EU contain a number of critical vulnerabilities for personal and business data transmitted to a cloud computing infrastructure. Therefore there is the need of adapting and creating standardised implementations to safeguard the security and privacy requirements against failures and attacks. Related to these security and privacy requirements, the EU legal framework provides basic conditions which apply for processing of personal data. However, the allocation of legal responsibilities may prove difficult in real-life cases, where a multi-layered involvement of several parties, render the transparency in regard to the whole infrastructure and the single actions of said parties almost impossible. The TClouds project aims at providing an EU law compliant secure and resilient cloud computing environment prototype while focusing on privacy protection for cross-border usage of cloud services. It targets an end-user friendly, transparent and easy to use system which allows the widespread use of virtualised IT-services while resolving the main concerns about delegating sensitive data or critical infrastructures into a cloud computing environment. Within the scope of this project, we hereby present the design of an exemplary and preliminary role model, which aims at achieving a common understanding of the different roles comprised by various cloud computing scenarios. The objective is to sketch a general infrastructural overview while approaching the critical problem fields of cloud computing.

8.2 The architecture of cloud computing infrastructures

The composition of cloud computing systems determines certain functionalities which lead to the representation of these functionalities in factual roles of the involved parties. So to understand these different roles in this special IT infrastructure, it is necessary to have a closer look at the general design of exemplary cloud computing systems.

8.2.1 General definition of cloud computing

Cloud computing emerged as an architectural and workload-wise shift from local computing resources to a network of computers designated to the delivery of IT services. It enables the use of these services as pay-as-you-go-supply via the internet instead of storage and use of these IT services in a centralised local computing environment. This remote demand for data processing occurs via the terminal access leveraged only by the local web browser or a thin client. Therefore, cloud computing infrastructures are an offer of internet-based IT services

tailored to suit a market need, which are provided as storage, computing power, development environment, application or even complete work environment services. Therefore, cloud computing can be defined as a model for enabling convenient, on-demand network accessed computing resources, in the case of a public cloud provided by an external entity. Numerous enterprises already resort to cloud computing for outsourcing complete work processes or timely covering peaks of demand which the own IT infrastructure cannot handle. Private persons also have the possibility to use IT services from the cloud. Many people already use cloud services without being aware of it, for example via web-based email and image storage services. This approach is not only of interest for potential customers because of the imminent cost efficiency, but also because of the possibilities of location-independent access to the data as well as the dynamic scalability of IT infrastructures.

8.2.2 State-of-the-art in cloud computing architectures

Cloud systems usually consist of different deployment types. These deployment types are the private cloud, the community cloud and the public cloud. The Private cloud is usually enterprise owned or leased. The cloud infrastructure is operated solely for one single organization or several, consolidated companies. It may be managed by the organization itself or a third party. The community cloud is a shared infrastructure for a specific community. It can be shared by several organizations and support a specific community that has common concerns (e.g., mission, security requirements, policies and compliance considerations). It may be managed by the organizations or a third party. The Public cloud is generally understood as a cloud infrastructure which is made available to the general public or a large industry group and is owned by one or more organisations selling cloud services. If these deployment types are combined into a composition of two or more clouds (private, community, or public), it is called a Hybrid cloud, in which the single clouds remain independent entities but are affiliated by standardised or proprietary technology that enables data and application portability [NIST].

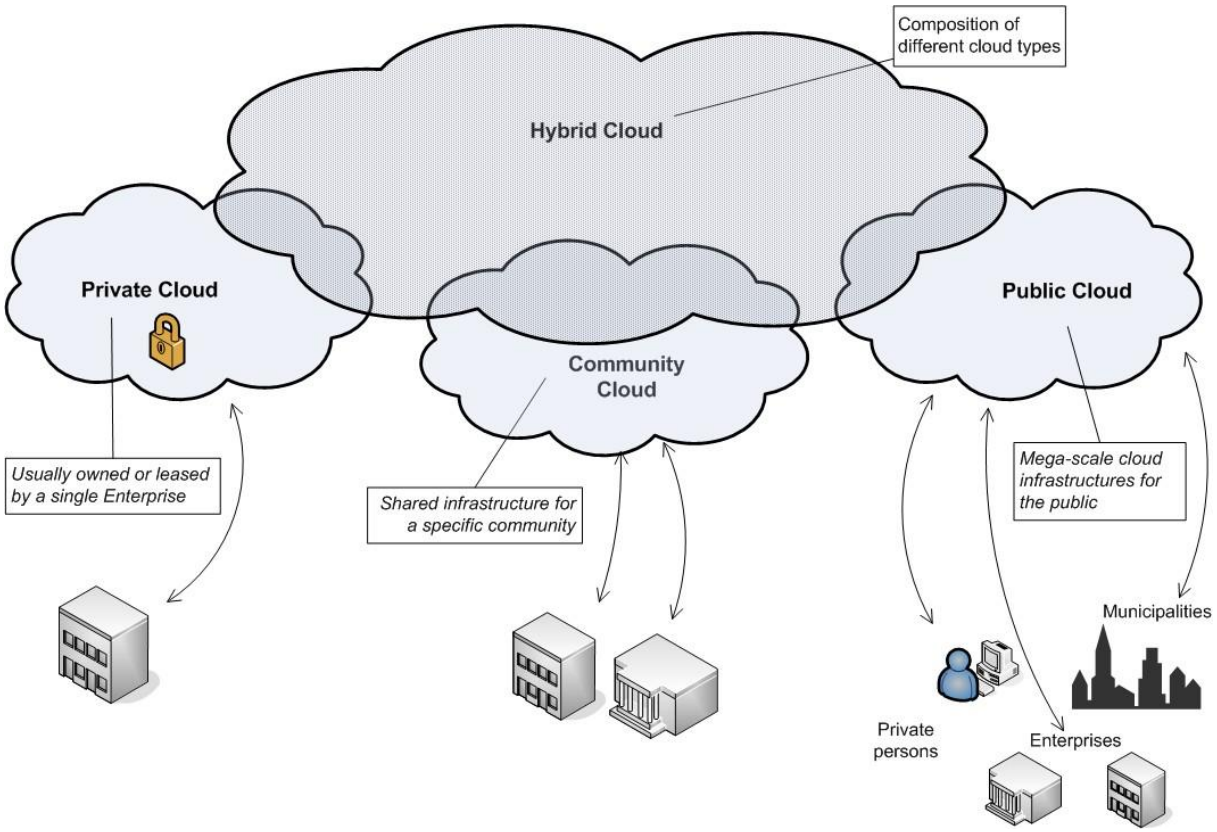


Figure 5: The four deployment types of cloud computing

Although there are almost no standardised structures specifically for cloud computing infrastructures yet, three basic service models that accompany the deployment types have been consistently identified by IT experts. These service models are infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service (SaaS).

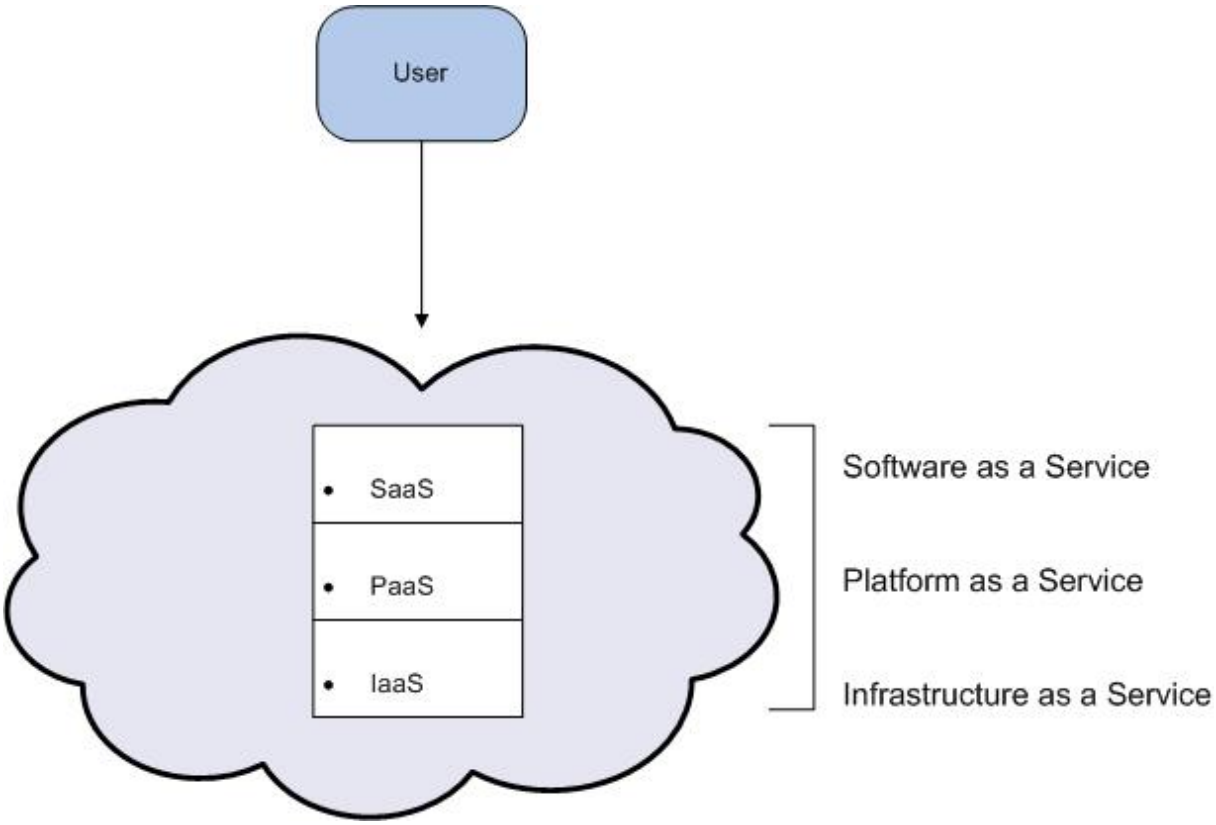


Figure 6: Common service models of cloud computing

Prominent examples for these service models are Amazon.com Inc. (Amazon) with its Elastic Compute Cloud (EC2) for IaaS, the Windows Azure hosted platform for PaaS and Salesforce.com for SaaS. But although these three service models are often used to describe the service layers in a cloud system, they are too coarse and too technically oriented to deploy all inherent legal and business aspects of possible services and implied roles in a cloud computing infrastructure. In the Windows Azure Services Platform, which is generally classified as a typical PaaS system, a closer look reveals a lot more implied roles than just the provision of a hosted platform. In the first instance, Windows Azure offers classical PaaS such as computing power and storage of data. But it also provides the customer with a number of services, which alleviate the creation and implementation of applications by the customer. For example, the Windows Azure AppFabric Service Bus connects in-house applications and services in the cloud, regardless of where and in which programming language they were created.

Nevertheless, there are even more aspects regarding the service provisions and implied roles in the Windows system. The above mentioned Service Bus does not only connect applications and services, it also provides an access control management for the customer. Another offered service is the Windows Azure Fabric Controller, an extensive management layer which is built-in to control and monitor the offered platform services and to enable the implementation of new services. Therefore, it is a comprehensive management subsystem with several defined functionalities. The Windows Azure cloud system also offers further services, such as messaging (Live Services), web portals (SharePoint Services) and dynamic CRM services. Internally, all these on-demand services must deploy a mandatory metering which is necessary for the usage-dependent billing. Other implied services are thinkable, for example security, flexibility and availability management.

Beyond these three service models, the architectural structures of cloud systems generally have an integrated cross-layer management called Middleware, which allows the connection

between the networked computers, layers and components. Depending on the different vendors of cloud computing, this Middleware can have the various add-on functionalities, such as fault-tolerant security automatisms as well as automatisms for synchronising and monitoring the cloud capacities.

As a conclusion, the general labels of IaaS, PaaS and SaaS plus the associated management layers of the cloud are not sufficient to depict all the numerous provider services which are tied to the central service offer. Instead, it is necessary to depict the various services, respectively their providers in their specialised roles in more detail. To take a closer look at an exemplary IaaS Infrastructure and some of the inherent roles, Amazon's Simple Storage Service (Amazon S3) is an adequate example. Amazon is a leading provider of IaaS cloud services and therefore has to be considered in regard to the current state-of-the-art. Though Amazon's Elastic Compute Cloud (EC2) is more popular, due its simpler architecture S3 is more convenient to give an overview of some inherent roles.

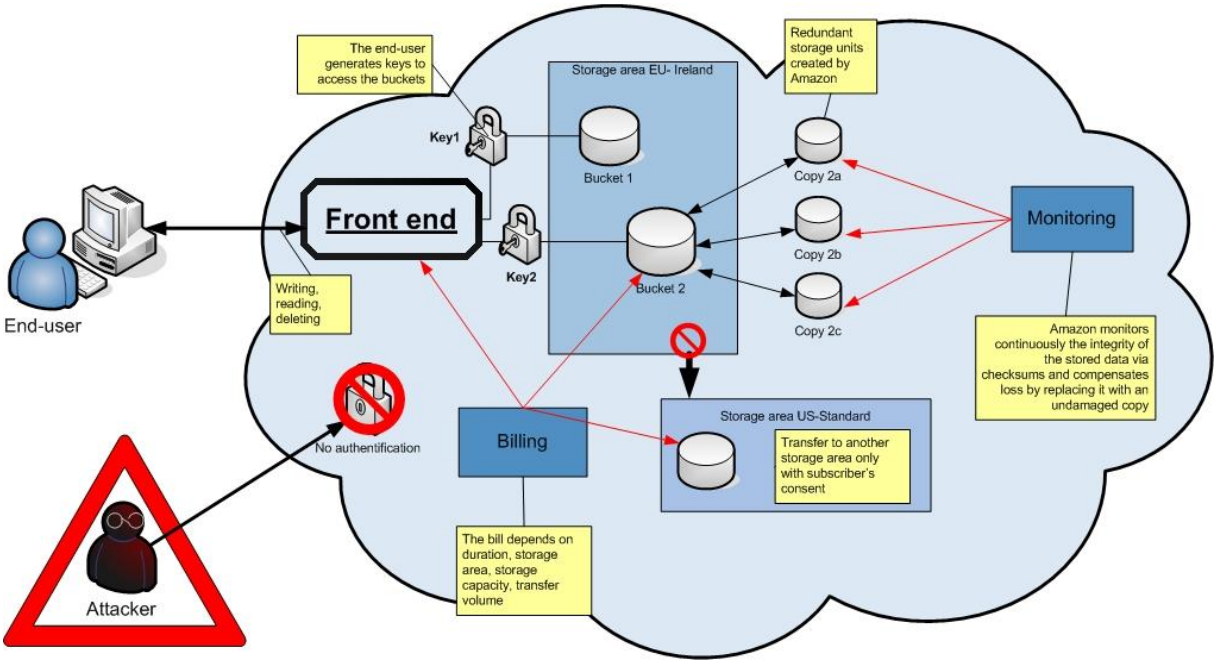


Figure 7: Amazon S3

Amazon S3 offers storage space. The end-user can enter his data into an application front end and the save the data in a so-called "bucket", a storage unit. This front end is the single point of contact, where the end-user can enter, read, change, overwrite or delete his data. When he assigns Amazon to store the data, he has to generate keys to restrict the access to the buckets as well as choose a storage area. Amazon offers four storage areas and obligates itself by its policy not to transfer data from the chosen storage area to another without the subscriber's consent. During the transfer and storage of the data, Amazon creates checksums for the data and continuously monitors via this checksums if the data has been corrupted. In the case of loss or corruption Amazon replaces the corrupted data with an undamaged copy. Therefore, Amazon stores an unstated number of copies of the subscriber's data on different devices.

Amazon bills its customers dependent on the capacity of the stored data, the chosen storage area, and the duration of the storage and the volume of data transfers (which occurs every time a bucket is retrieved to work with the comprised data).

At the basis of this coarse description some exemplary roles in the sphere of the cloud service provider can already be identified, though in the case of S3 all of these roles are administered by Amazon:

Access rights management provider: Amazon offers its customers the opportunity to create keys to restrict the access to specific buckets for a certain group of end-users. Furthermore, the customer can demand that certain end-user group shall have only restricted rights in regard to specific buckets, e.g. read-only-rights. The access rights management provider has to ensure that the security measures are in place and that only the authorised end-user can access the data and that he is only allowed to execute the constituted operations on the data. The access rights management provider therefore has to process data regarding the identification of the possible end-users on behalf of the customer. Dependent on whether the authentication of end-users needs personally identifiable data, the role of the access rights manager might be data collector or data processor in regard to the authentication data.

Monitoring provider: As stated above, Amazon continuously monitors the checksums of the customer's data and all copies and will intervene if the checksum of one copy differs [S3 FAQ]. This procedure might become critical in regard to business relevant or personal data, if the checksums allow conclusions about the real data as well as monitored changes of the data allow conclusion concerning the access and therefore working hours of the customer. In both cases the monitoring would have to deal with personal data and has to be considered a data controller. This applies regardless of whether the monitoring is done completely automatically or not, because even for an automated process, there has to be a responsible party. The monitoring process might also be critical in the conceivable case of unwanted repair of the data. Because the exchange occurs without the customer's awareness or consent, an erroneous exchange of copies might run counter to the customer's interests and even lead to data loss.

Billing provider: To be able to address the bill, Amazon has to collect the contractual data of the customer. But in accordance to Amazon's policy, the user is charged for a pay-as-you-go service which necessitates the collecting of detailed traffic data, such as capacity of the stored data, the chosen storage area, the duration of the storage and the volume of data transfers. This traffic data allows extensive conclusions on the behaviour of the end-users and is therefore critical in regard to data privacy aspects. Amazon in the role of the billing provider acts as a data controller.

These three exemplary roles already show the variety of different duties and responsibilities within a cloud service infrastructure. In a conceivable more complex scenario, in which all of these roles are impersonated by different legal entities, each of them would have different legal and contractual liabilities. Therefore, to create a comprehensive role model, which applies to most cloud service models, all possible roles have to be analysed. The following chapters will endeavour this approach to achieve a better understanding of the roles of the involved parties in a cloud computing infrastructure. Besides the roles within the sphere of the cloud service provider, all external roles possibly affecting the data stored in the cloud or even the model of cloud computing as a whole must be analysed.

An example for the complexity of current cross-border data processing in regard to European customers is the SaaS cloud service of Salesforce.com. Similar to Amazon, Salesforce.com is one of the market leaders for software applications in the cloud computing field. Salesforce.com offers its customers various applications, one of them a prominent service for Customer Relationship Management (CRM). Salesforce.com is a US company; all of the

hardware for the provided cloud infrastructure is located within the US. To allow European customers to use the cloud services while trying to elude the strict European legal requirements for transfer of personal data, salesforce.com established a system of subcontracts.

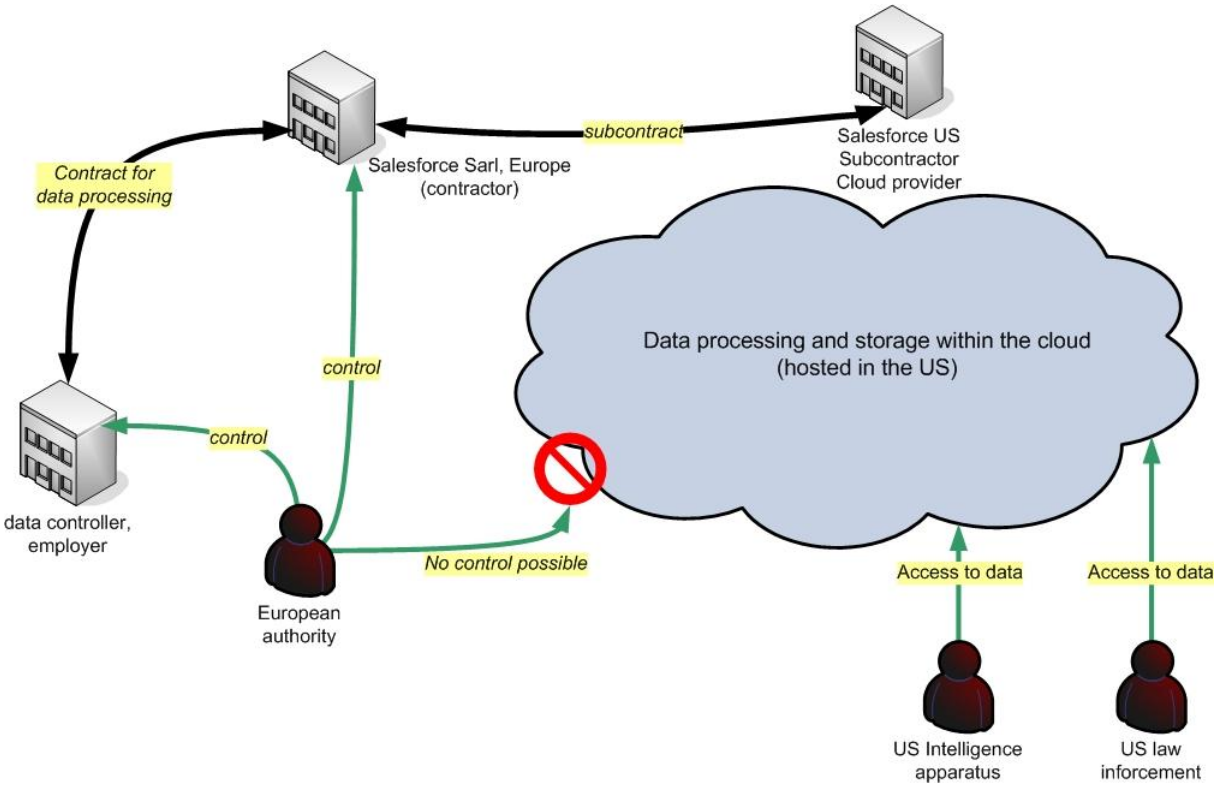


Figure 8: Salesforce.com

The European customer concludes a contract for data processing with the legally independent European subsidiary company Salesforce.com Sàrl, located in Swiss. In the case of the customer being data controller, Salesforce.com Sàrl therefore becomes data processor in regarding the personal data. It furthermore concludes a subcontract for data processing with Salesforce.com Inc. in the US with the consent of the customer; Salesforce.com Inc. therefore becomes a sub-processor in regard to the personal data. The customer then simply uses the cloud services of salesforce.com like any US customer.

Salesforce.com states that due to being compliant to the Safe-Harbor-Principles, a data transfer to the US is allowed without the information and consent of the concerned data subject. So the information of the data subject, e.g. a customer of the European data controller, would be dispensable because the actual contracting party is a European company. Regardless of whether this legal appraisement is correct or not, it might lead to the objectionable outcome that without the data subject's awareness, his data might be processed within the US. Due to the anti-terror-legislation, e.g. the US Patriot Act, the US intelligence apparatus, homeland security and law enforcement authorities have capacious access authorisation in regard to all data held on U.S. located servers. As opposite to the US authorities, European ones, though competent for the European customer, have no possibility to access the data or control the data processing.

As this example of Salesforce.com shows, subcontracting and outsourcing of tasks is already an oftentimes deployed reality in cloud computing. Therefore it must be considered that most of the following cloud provider roles might as well be impersonated by subcontractors.

Furthermore, it must be considered that in cross-border cloud computing scenarios foreign authorities and other parties might be authorised to access the data processed within the cloud.

8.3 Overview of roles

This report aims at conveying a general role model, which can to some extent apply to most cloud computing service models. Therefore, in this chapter, a survey of the different roles in the cloud computing system will be made. However, it is not laid out as a detailed role model for the highly specified use cases in the eHealth and energy sector selected for the TClouds project. The elaboration of such precise role concepts in the context of such use cases will be conducted in the later reports of the project. Furthermore, the contemplation of the general roles introduced in this chapter is solely functional and do not comprise a legal evaluation of their interactions and resulting responsibilities. This legal evaluation will also be part of later reports in this project.

To aim at a more defined margin of roles, the division of the involved parties into different spheres is essential. Therefore, on the basis of their relation to the cloud infrastructure, the division into four basic role spheres is mandatory. These are the four superordinate spheres or concepts of:

1. the subscriber sphere;
2. the cloud service provider sphere;
3. the connection and access sphere;
4. and the sphere of other possible influences, which are external but still related to the cloud in the broadest sense.

These spheres are the coarsest distribution of involved parties to begin with.

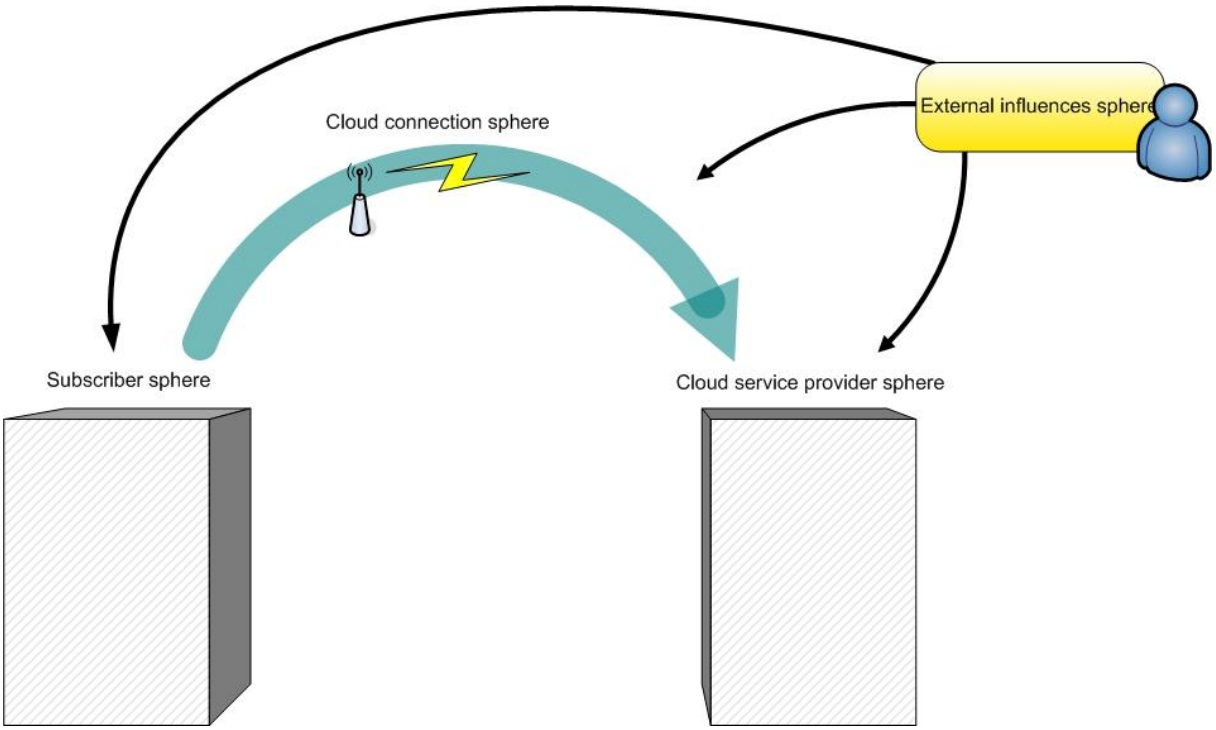


Figure 9: Overview of Spheres

The first superordinate concept in a cloud computing infrastructure shall be the subscriber sphere, consisting of various roles that use the cloud, ranging from a subscribing company with its employees to the common end-user who subscribes to a cloud-based email-service. Counterpart of this sphere is the cloud service provider sphere. It also consists of several inherent roles and might be represented by numerous legal and natural persons. To use these cloud services, the subscribers need to have connection to the cloud. This connection is achieved by a networked inter-linkage, which in case of a public cloud could be an internet-based admission provided by an Internet Access Provider (IAP) and in case of a private cloud an in-house network provided by a network access provider. Beyond these aforementioned spheres, other external influences can have under certain circumstances a direct impact on the cloud infrastructure and the involved parties. These external influences are e.g. policy makers, investigation authorities and attackers.

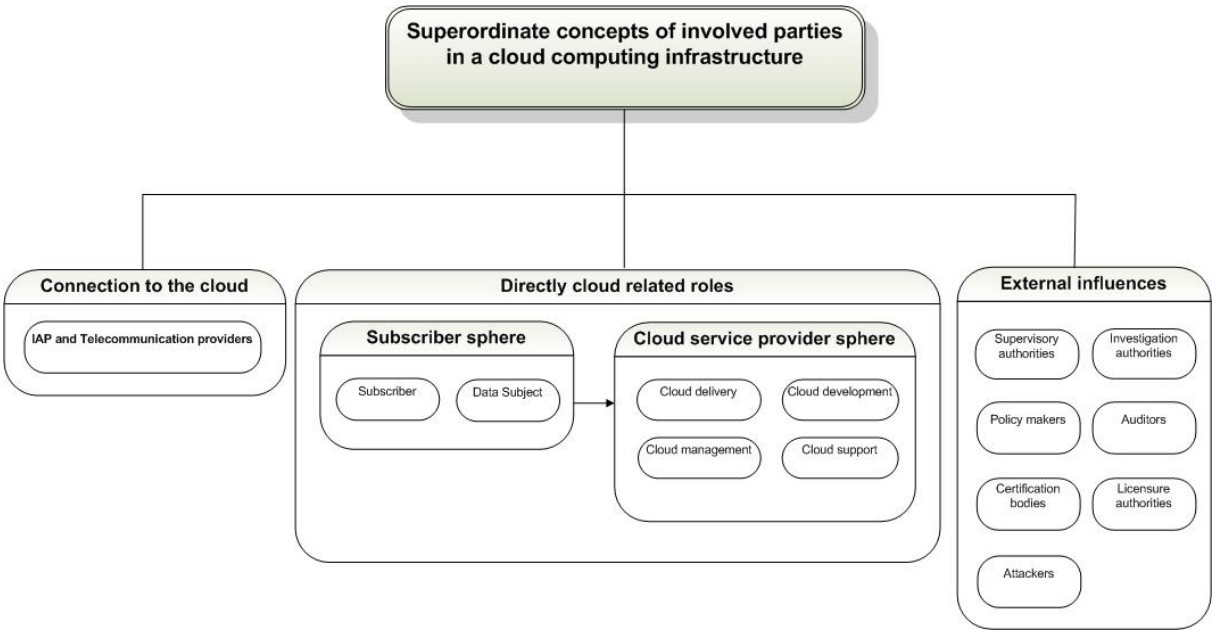


Figure 10: Overview of superordinate concepts

8.3.1 Subscriber sphere

As said before, the subscriber sphere can imply a number of different roles embodied by diverse parties. Which natural or legal person has to be categorised into one of these roles, depends on his or her significant de-facto position and activity related to the usage of cloud services. These roles are:

1. Subscriber;
2. Data Subject;
3. End-user;
4. Dependent end-user;
5. Account holder;
6. Concerned legal person;
7. Local infrastructure provider.

8.3.1.1 Subscriber

If the active party, who uses the cloud service in order to process data, is contractually connected to the provider of the cloud service, it shall be named subscriber. This applies regardless of whether the service is free of charge or not and whether the contract is written down or inferred from acts of parties. The subscriber might either be a natural or a legal person. If the subscriber holds the authority to decide the purposes and means of the processing of personal data he also holds the role of a data controller; the cloud service provider will in most cases hold the role of the data processor on behalf of the subscriber. If the subscriber is a legal person, it regularly is data controller for data related to its employees. For example, regarding a human resources management (HRM) application being run in the cloud, a company is data controller regarding the personal data of its employees. This may also apply to a company's customers personal data insofar as the company collects and processes this data for the purpose of billing or customer relationship management (CRM). Other constellations are thinkable, such as personal data of personnel of affiliated companies or just potential customers and business partners. The key element to

classify the role of the subscriber must always be the utilisation of a service to handle personal data.

8.3.1.2 Data subject

The natural person whose personal data is being processed shall be denominated data subject. The two roles of the subscriber and the data subject might be embodied by the same natural person, e.g. in the case of an end-user who subscribes to an IaaS cloud service to store his personal documents. Then again the subscriber may as well be a legal person whose employees use a SaaS cloud service to manage their customer relations. In this case the data subject, thus the customer of the subscriber, does not necessarily have a direct access to the cloud on his own.

8.3.1.3 End-user

Another important differentiation needs to be made between the subscriber and the end-user. Whilst the subscriber may either be a legal or a natural person, who has contractually subscribed to the cloud service, the end-user may only be a natural person who actively uses the provided service. In the case a company subscribes to a cloud service, the company itself, as a legal person, might not be denominated as an end-user. Rather, the employees of this company who actively employ the service are the end-users in this scenario. Dependent on whether their own personal data is processed, e.g. for HRM purposes, the end-users are data subjects as well.

8.3.1.4 Dependent end-user

Depending on whether the end-users themselves may decide on the circumstances of the data processing or not, they shall be denominated dependent end-users. If the subscriber is a legal person, only the natural persons working for this legal person are actually able to be end-users of the provided service. Because these natural persons will oftentimes be bound by instructions of the legal person’s policies, they might be called dependent natural persons. Commonly, the policy of a company will determine purpose and means of the data processing by its employees. If data is processed in the cloud by the employees as dependent end-users, the subscribing company's employees are as well data subjects of e.g. the billing and logging providers of the cloud service.

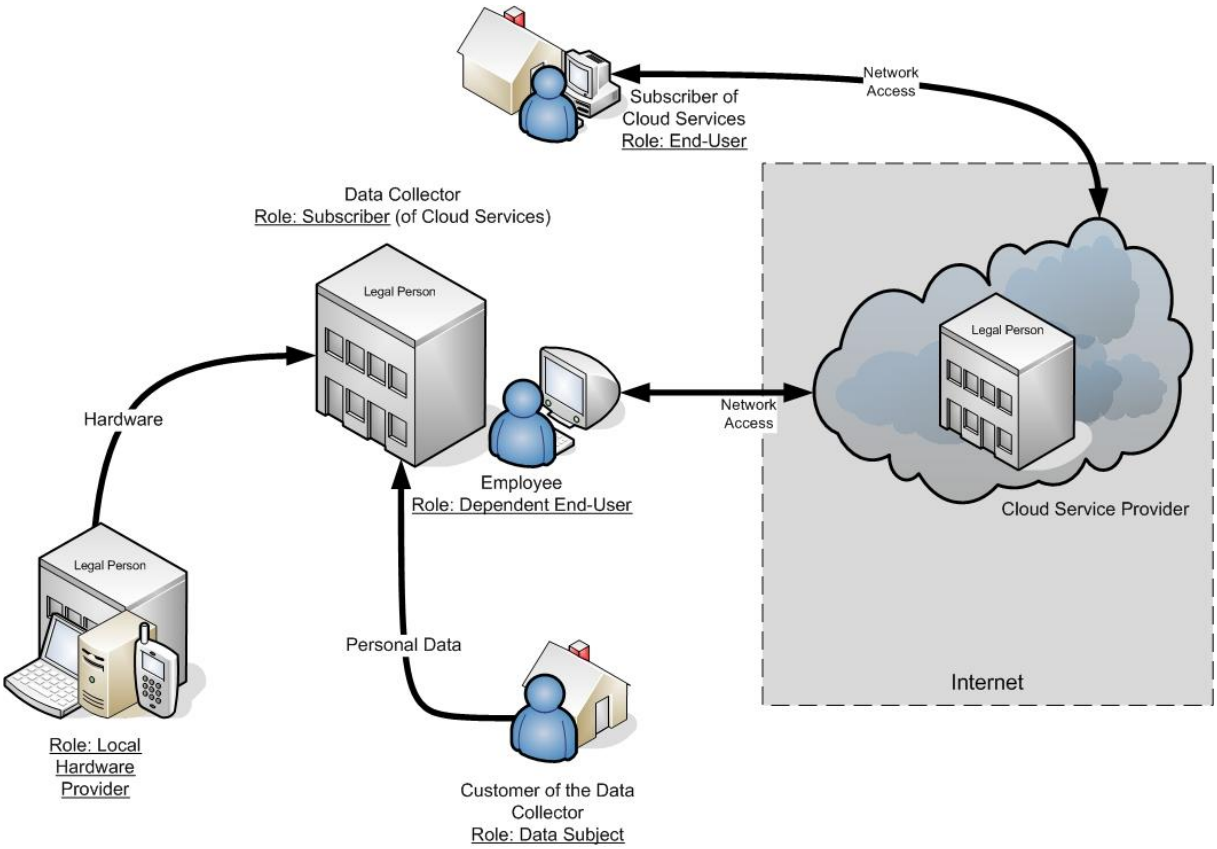


Figure 11: Figurative Role model of the subscriber sphere

8.3.1.5 Account holder

There needs to be considered that there might exist a party who is not an active end-user but owns an account of a cloud service. This account holder does not necessarily be subscriber of the service. Even though this role of an account holder might seem dispensable at first sight, it is not uncommon that the subscriber creates accounts for some natural or legal persons. E.g. the subscriber to a customer relation management cloud service might create accounts for all of his customers, so that the customers can update their personal data by themselves. These customers would be account holders without needing to use the account or without even knowing about the existence of the account. By generating these accounts the account holders might become a data subject, dependent on whether personal data is required for the account generation. As a result the party who decides on the purpose and means of processing the account data will become the data collector regarding this data. The deciding party might either be the subscriber or the respective cloud service provider or both of them jointly.

8.3.1.6 Concerned legal person

In case of cloud computing we face the situation that not only individuals but also legal persons might be the subject of data processing. If we recall the scenario of a subscriber company which processes customer data in the cloud, these concerned customers might be natural persons as well as legal persons. Since the EU Data Protection Directive states that only natural persons might be named data subjects, this legal person has to be denominated as the concerned legal person. Though this concerned legal person can not be subject of rights regarding "personal" data, it is nevertheless protected by article 8 of the European Convention on Human Rights (ECHR) regarding notably its industrial secrets, its know-how

and other sensitive business information. Of course, the employees of this concerned legal person might still be data subjects, in case their personal data is being processed.

8.3.1.7 Local infrastructure provider

It also might happen that the subscriber outsources his local IT provision and care to an external party apart from cloud computing IaaS providers. Depending on the contractual obligations, this local infrastructure provider might have to take care of the local security measures and other important means regarding the use of cloud computing services.

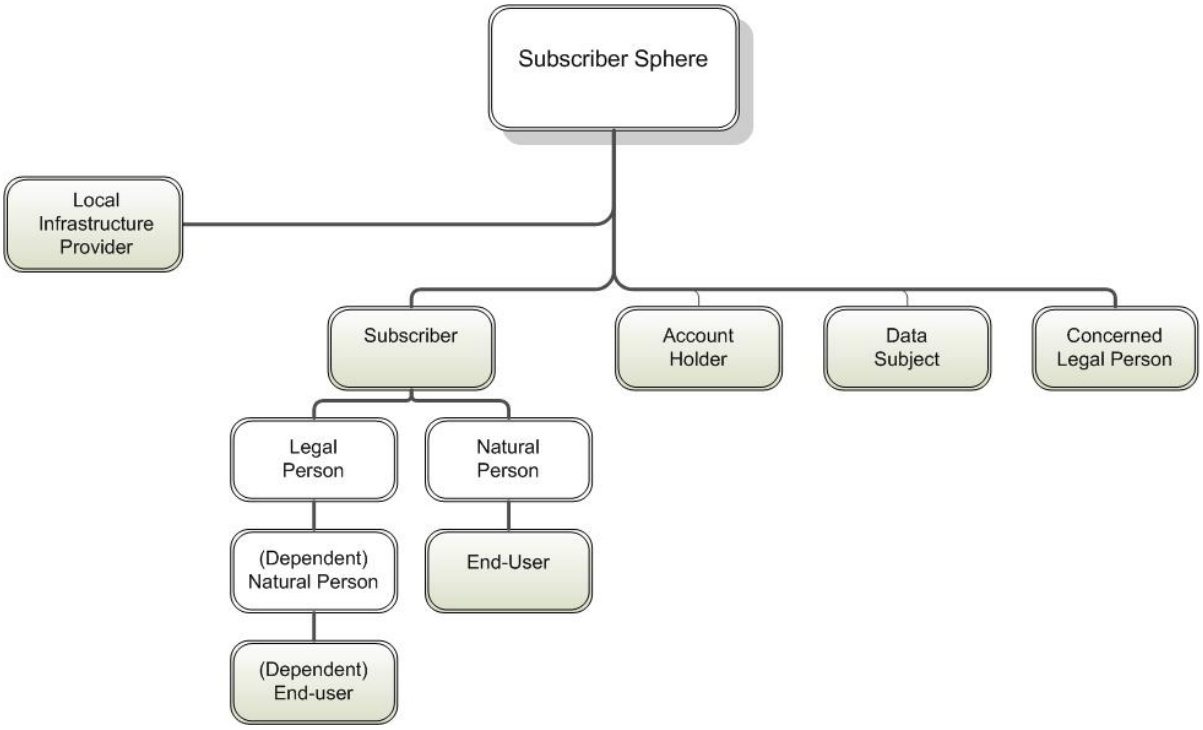


Figure 12: Role model of the subscriber sphere (actual roles are highlighted)

8.3.2 Cloud Service Provider sphere

Within the sphere of the cloud service providers, a functional division of service providers is required. First, the cloud will be developed and implemented by IT professionals and then operated by the delivery entities. Subsequently, the overall management of the cloud services is usually accompanied by the cloud support. Therefore, we have the following cloud service provider entities:

1. Cloud delivery;
2. Cloud Management;
3. Cloud support;
4. Cloud development.

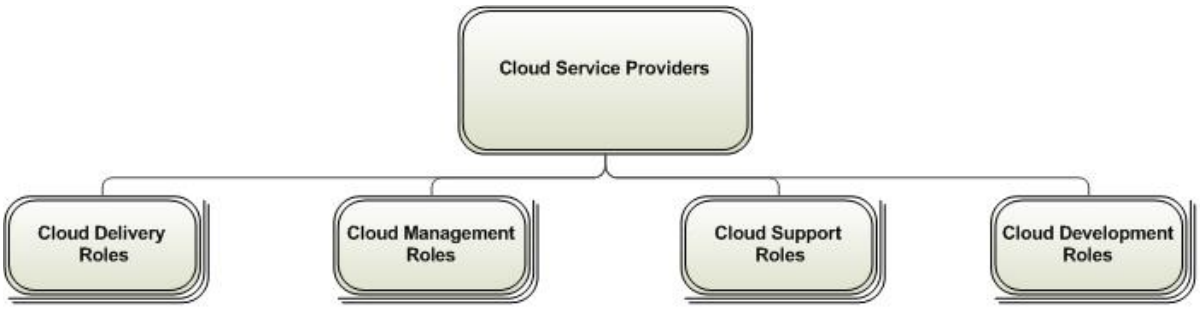


Figure 13: The four Cloud Service Provider entities

The cloud delivery section defines the front-end of the cloud service. All applications, functions and services which are directly visible to the customer and have market-value for the cloud service provider are comprised there. This front end is facilitated by the cloud support, which includes all roles that are responsible for providing and maintaining the technical support of all services in the so called back-end of the cloud. The cloud management coordinates the cooperation and interworking of all spheres. It is also competent for the business management as well as the contact to customers. The cloud development is the elementary basis for the cloud structure itself. It is concerned with the programming, designing and implementing of components.

Furthermore, some external entities, which have an immediate contractual relation to the cloud service providers, have to be included. These are:

1. Subcontractor;
2. Supplier;
3. Reseller.

8.3.2.1 Cloud delivery

The cloud delivery comprises of different services that are offered to the subscribers and end-users directly. This encompasses services like hosting, storing, computing power, applications etc. These are the services that are directly accessible for the subscriber and end-user via the front end of the cloud. They are also the relevant core services with immediate market value in the cloud infrastructure. For the customer, the provisioning of a service with quality, dependability, cost-efficiency and privacy/security is part of the crucial decision criteria to enter a contractual agreement with the cloud service provider.

The range of offered services in this branch of business and the possible affiliated individual contracts specifications are broadly based. Therefore, it is not feasible to depict the roles of the Cloud delivery section and their corresponding functional responsibilities in an all-embracing manner. These must be contemplated and determined anew in every singular case for every single provider. This also applies to the question if a cloud delivery provider is to be considered data controller or data processor. Nevertheless, several exemplary Cloud delivery roles shall be contoured to give a conception regarding the variance of offered services.

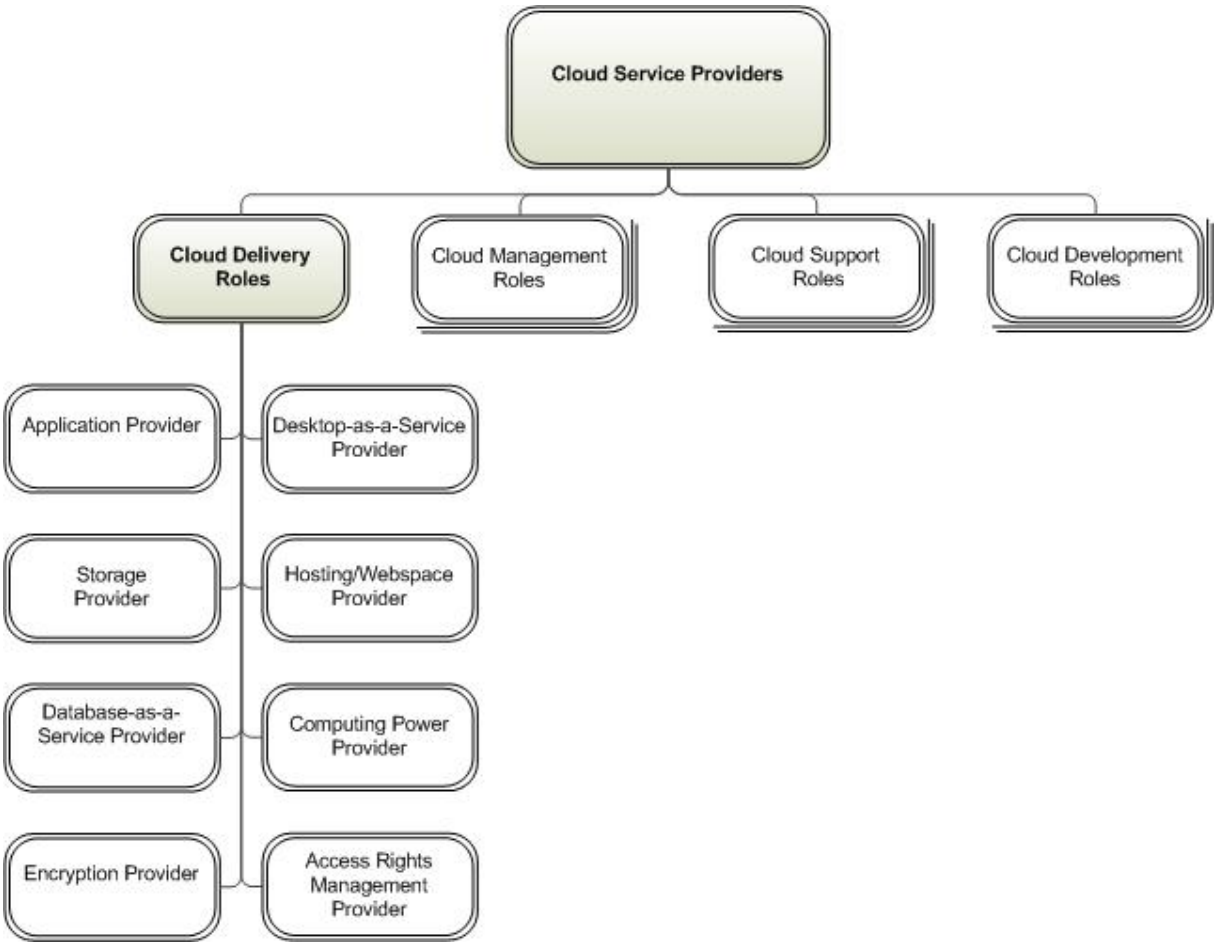


Figure 14: Cloud Delivery Roles

Many of these roles may be incorporated by one or few providers at once because many of these services are based upon each other, work jointly together or are simply part of a broader product range of a service provider.

8.3.2.1.1 Application provider

The Application provider offers IT software for users, which may enable them to carry out a certain assignment of tasks. Examples are the SaaS provider in a cloud system, which offers enterprise IT solutions such as Human Resources (HR), Enterprise Resources Planning (ERP), Accounting, Office suites. For private persons, the use of media players, graphics software or web-based email services are prominent examples.

8.3.2.1.2 Desktop-as-a-service provider

The Desktop-as-a-service provider offers a virtualised desktop environment originated from a remote server. The subscriber can access the desktop including the remotely installed programs and applications from any location with an appropriate device.

8.3.2.1.3 Storage service provider

The storage provider offers memory capacity. The storage service provider may also offer backups and archiving of stored data with the aid of associated application programs.

8.3.2.1.4 Hosting/Webspace provider

The Hosting provider enables his customers to host the programmed applications and also run these on the hosted platform. In contrast, a Webspace provider offers his customers the mere webspace with just a very limited possibility to run own applications.

8.3.2.1.5 Database-as-a-service provider

The Database-as-a-service provider is offering its customers mechanisms to create, store, and access their databases in the cloud. He basically offers a composition of other cloud delivery services, such as storage, hosting and the provisioning of hardware as well as, depending on the service model, software applications which allow specific operations on the database.

8.3.2.1.6 Hardware environment provider

The Hardware environment provider will make hardware devices, components or complete facilities available for use by the subscriber. Therefore, he provides the most basic functional equipment for processing IT workloads.

8.3.2.1.7 Computing power provider

The Computing power provider makes processing power for the execution of demanding computer work processes available to increase their work speed. Therefore, computing power is a means to improve the processing performance of programs.

8.3.2.1.8 Encryption provider

The encryption provider places mechanisms for data conversion into an encoded version at disposal for the subscriber. This service is meant to enable the subscriber to detract the content of his data from the active knowledge of unauthorised parties. This encryption service might be included in another service model either by default or voluntary. The technical and practical realisation of this service may be executed in various forms.

8.3.2.1.9 Access rights management provider

The access rights management provider enables the subscriber to restrict the access to the data in the cloud to certain groups of end-users. It allows the subscriber to define the rights a certain end-user has regarding the data, like e.g. being allowed to read but not to change the data. Therefore, the access rights management is responsible for providing adequate control mechanisms to safeguard that the defined restrictions are realised.

8.3.2.2 Cloud management

Aside from the core services, various management tasks need to be performed to ensure their regular operation. These tasks are established as a level of management functionalities. In many cases, single providers will adopt several or even all of these management functionalities, mostly by allocating automated processes to run in the cloud system. Usually, some of these functionalities are also embedded in the middleware to enable cross-layer resilience for the whole system and to provide an integrative and standardised management interface to handle interactions between providers of cloud core services and their customers and also deal with inquiries of potential third parties.

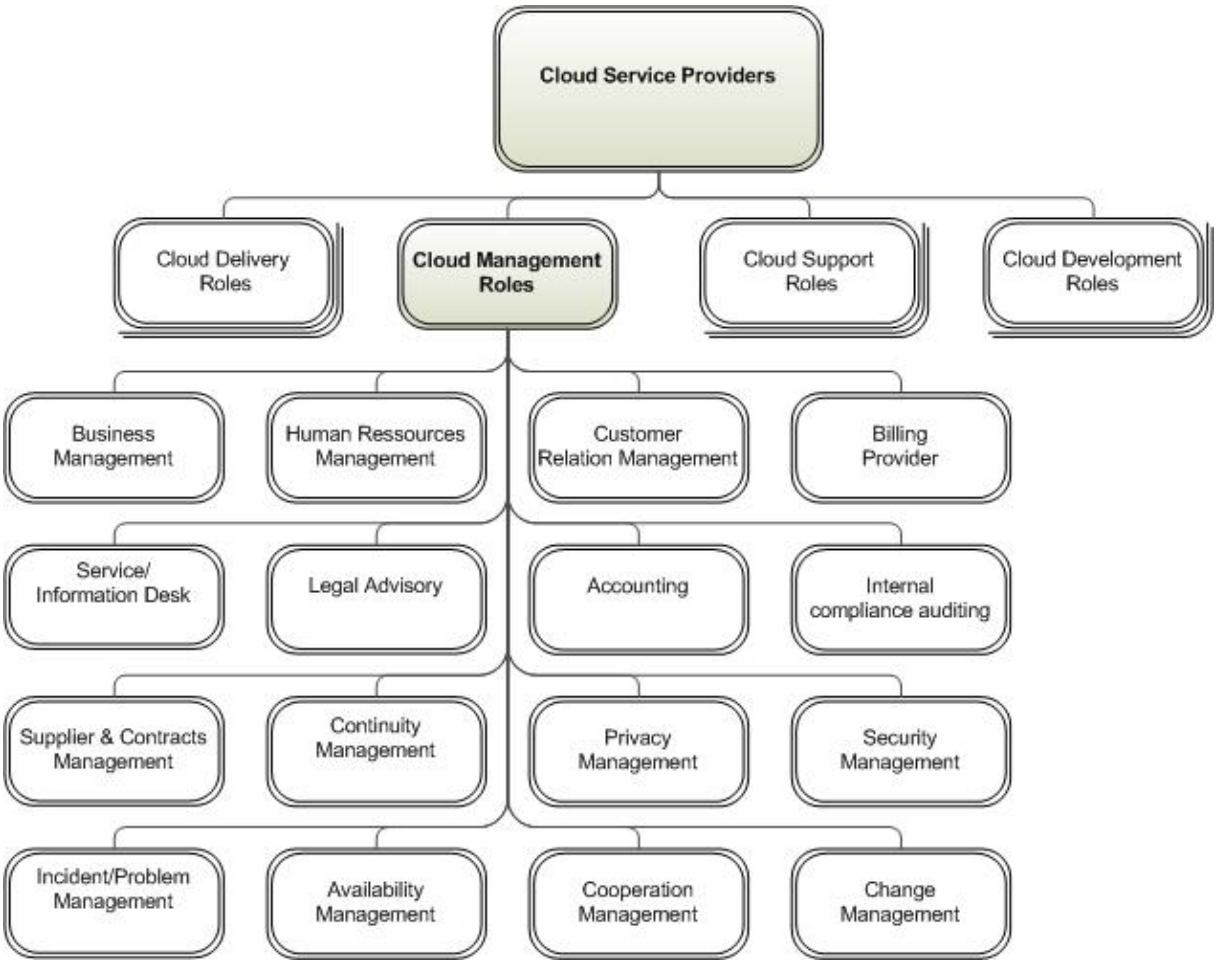


Figure 15: Cloud Management Roles

The inherent roles of the cloud management may be distinguished into the following generic classifications:

1. Core Management;
2. Directives Management;
3. Cooperation Management.

8.3.2.2.1 Core Management

8.3.2.2.1.1 Business Management

In context of this role model the business management shall mean the executive management of a cloud service provider. Dependent on the corporate structure of the company the form of organisation may vary, but this role concerns the overall responsible parties for business related decisions.

8.3.2.2.1.2 Human Resources Management

The Human Resources Management (HRM) executes the internal personnel administration of cloud service providers. Insofar as this management entity collects and processes personal data from the provider's employees, it is data controller.

8.3.2.2.1.3 Customer Relationship Management

The Customer Relationship Management (CRM) aims at a smooth interaction with the customers and end-users to ensure the utmost efficient administration of service demands and their realisation. Another main task of CRM is to spot and attract new customers. The overall organisation of the relations with customers might include the recording and monitoring of all interactions with the customers. This concerns especially interactions with the service or information desk.

8.3.2.2.1.4 Billing Provider

The billing provider charges the customer for the usage of the provided cloud services. Since a characteristic trait of cloud services is the pay-as-you-go billing, it is often necessary to collect not only contractual data to identify the addressee of the bill but also the traffic data of the end-users. This traffic data might include several fields of data which might be accumulated to a detailed idea of the end-user's behaviour. Dependent on how circumstantial the pay-as-you-go service is determined, the billing provider might have to collect data concerning the specific end-user access rights, the date and time of his access, the accessed file's size, duration of data transfers, location of data storage, terminal equipment etc. Therefore, the billing provider personates a data controller or at least a data processor on behalf of the data controller who decided on the amount and means of the data needed for the pay-as-you-go billing.

8.3.2.2.1.5 Service/Information Desk

The Service and/or Information Desk deals with service requests and demands of external parties. These might be customers as well as e.g. law enforcement authorities which want to access the traffic data as potential crime evidence. This role is also the contact point for subscribers and end-users of the service if technical problems occur. In case the service/information desk needs to collect and process personal data to answer these requests or forward them to other roles, it becomes a data controller.

8.3.2.2.1.6 Legal advisory

The legal advisory, regardless of whether internal or external, is mostly responsible for developing and adjusting the cloud service policies and the service contracts with the cloud customers. Therefore, the legal advisor needs to be well-informed about influences of legislative and law court decisions regarding the requirements for the established contracts and policies.

8.3.2.2.1.7 Internal compliance auditing

The internal compliance auditing of the cloud system assesses the mandatory external requirements as well as the specifications of internal policies that must be met by the current condition of the cloud parties, facilities and organisation. These requirements could be of legal nature, such as law restrictions regarding data collecting and processing within the cloud. But they could also be of economical nature, such as the effectiveness and optimisation of internal workflows. This internal auditing role may also encompass further sub-roles such as an internal data protection commissioner or a youth protection officer. The auditing works closely together with the technical revisal to ensure the modification and further development of the system to align it with the stipulated requirements.

8.3.2.2.1.8 Accounting

The Accounting carries out the general administration of financial issues. This administration gets carried out via a chronicle of all financial business transactions on the basis of bills and receipts. This chronicle is a reflexion of the provider's economic resources measured in purchasing power or in monetary units. Depending on the internal organisation of the business transactions, the accounting provider may have access to the data collected by the billing provider as well as data collected by the supplier and contracts management.

8.3.2.2.1.9 Supplier contracts management

It is conceivable that the cloud service providers receive their hardware and other resources from an external supplier. The contracts with numerous possible suppliers have to be managed by a responsible party within the cloud provider sphere. The contracts have to be controlled and adjusted frequently to avoid unwanted limitations and indemnities of liability and to minimise or even eliminate objectionable data disclosure toward the supplier. This role is also responsible to ensure complete erasure of own and customer data in the case of hardware disposal. The supplier management may rely on information given by the capacity management and other technical supervisory roles to coordinate the demand and the purchasing.

8.3.2.2.2 Directives Management

The internal technical management of the cloud infrastructure implies several functionalities which can be embodied in different roles. In most cases, these different technical roles may be incorporated by a single or few vendors and the provision of the implied services may concur jointly. It also may be that many of these technical services will be provided as automated processes.

8.3.2.2.2.1 Security management

The Technical Management includes a Security Management. However, this does not include the management of the physical hardware security, which is part of the cloud support. Instead, the Security Management on the technical level has responsibility for determining the cloud provider's corporate structure regarding the protection of the cloud networks and systems from unauthorised access and attacks. This does include the inventory of assets, risk analysis, risk treatment plan and the acceptance of residual risks [ISO27001, ISO27002].

8.3.2.2.2.2 Privacy management

The Privacy Management is concerned with the boundaries of data collection and processing. This role provides guidance in regard to the protection of the data subject's interests and the corresponding technical and organisational data processing procedures. In this context, it carries out the task of determining the legitimacy, necessity and appropriation of all collected and stored personal data for which the cloud service provider is either data collector or data processor. It might be represented by the role of the internal Data Protection Supervisor which can under certain circumstances be a mandatory assignment e.g. in Germany. The supervisory role may also involve investigating complaints lodged by staff members or any other data subject who feels that his personal data has been mishandled by the cloud service provider.

8.3.2.2.2.3 Availability management

The availability management monitors the accessibility of cloud delivery services and components. It furthermore controls their deployment, depending on their operational readiness and the stipulated policies. It then communicates the availability of services in response to subscriber requests. The availability management is therefore part of the service continuity as well as the fault-tolerance of the cloud infrastructure in favour of the customer. It usually has close connection to the services of capacity management as well as the monitoring/metering management from the cloud support section.

8.3.2.2.2.4 Incident/Problem management

The Incident/Problem management executes the ascertainment, analysis and action against compromises inside the cloud infrastructure. This implies the identification of events as not being standard operations of cloud services (e.g. denial of service (DoS) attacks, unwanted data loss etc.). It then is designated to commence amendatory actions, such as encountering the attack and restoring corrupted or lost data from backup devices. The Incident management also provides an interface for the subscriber to handle failures and resulting service requests. Just as the Availability management, this management entity will also overlap with monitoring/metering services from the cloud support section.

8.3.2.2.2.5 Business continuity management

The Business continuity management assesses internal as well as external risks and dangers. It then develops strategies, contingency plans and fall-back plans to safeguard the protection of the company's organisation, business activity, system integrity and also the integrity of the customer's data. Therefore, the Business continuity management is dedicated to prevent damages or losses in any cases of incidents as good as possible. In this context, the majority of such cases may be the bankruptcy or acquisition of the company and crisis situations caused by external criminal offenses.

8.3.2.2.2.6 Change management

The Change management role is designated to adjust services or single components of the cloud system within the boundaries of the affected provider's policies in response to change requests. These change requests may either come from the subscriber or from within the cloud provider sphere. A change management request of a subscriber may be issued on the basis of contractually stipulated Service Level Agreements or other legal obligations of the affected provider, which coercively bind him to react to specific events. A change management coming from the cloud provider sphere may come from various service providers, such as e.g. from the Security management, Availability management or the Capacity / Scalability management, depending on the nature of the precise issue.

8.3.2.2.3 Cooperation Management

The constitution of the cloud-internal cooperation management depends on the de-facto architectural structure of the cloud system. Two different constellations are thinkable in this context:

- In case of a federated cloud infrastructure, where several collocating clouds stand in equal relation to each other, the internal organisation is mastered by a cloud partner management entity.

- In case of a cloud system, where a superordinate cloud structure is involved to envelop the single sub-clouds of different vendors, this management will be undertaken by a meta cloud manager.

The internal organisation of the involved clouds and their vendors by these management services comprise not only the transfer of data between clouds and servers, but also the implementation of services offered by other participating cloud vendors. An example would be the SaaS provider who lets the own application run on the platform or infrastructure service of another vendor. This also implies the internal billing of underlying core services between providers.

8.3.2.3 Cloud support

The aforementioned cloud services necessitate further support services like hardware care and software maintenance & updates. This also encompasses the imminent physical security and hardware access control management. In most cases, the attendance to hardware and software will be entangled with the technical management for the cloud.

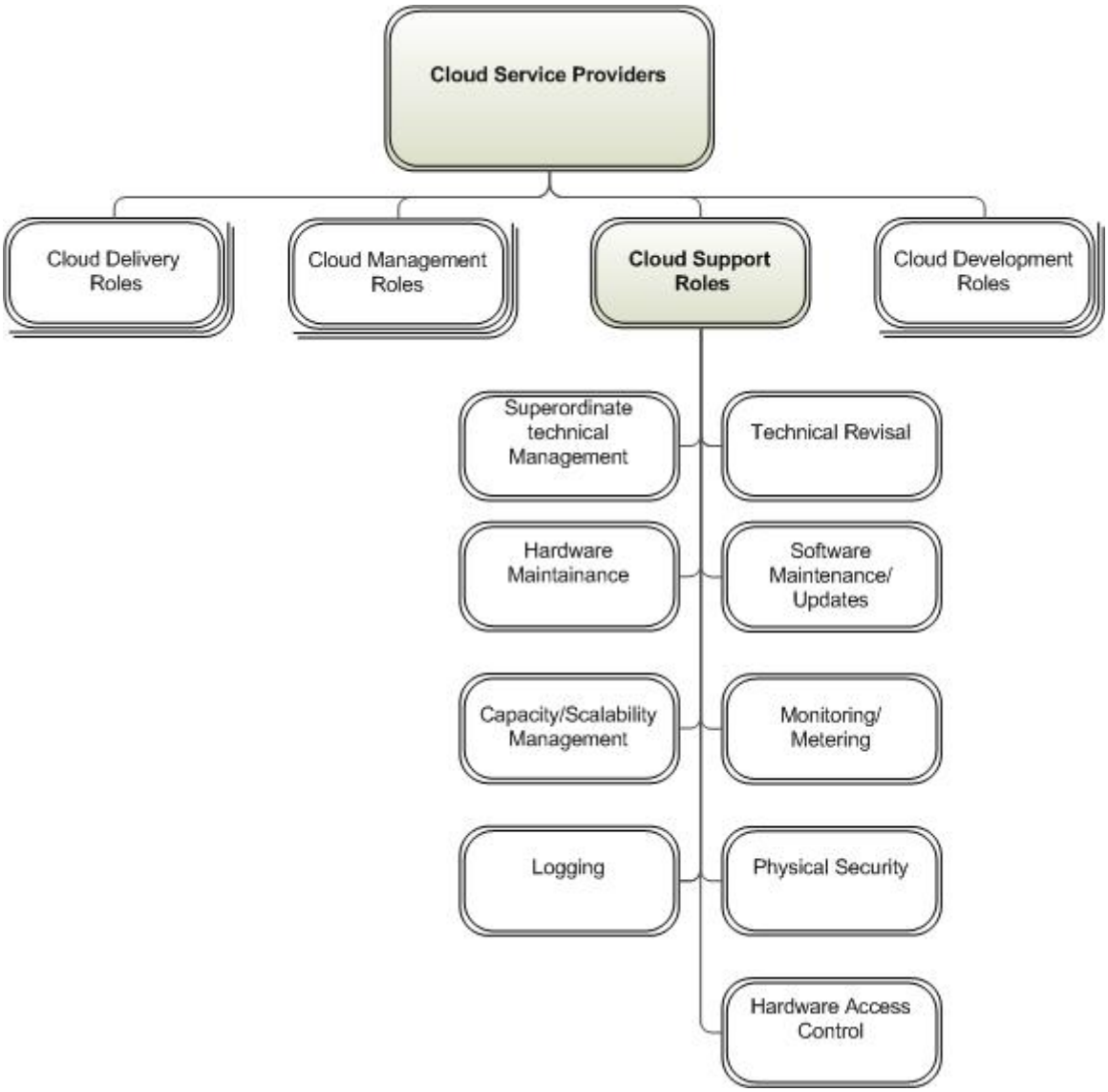


Figure 16: Cloud Support Roles

8.3.2.3.1 Superordinate technical management

The superordinate technical management is responsible for the general accomplishment of technical conversion. It decides on the means of operation, logistics, service and maintenance of the cloud system calibration. This management entity may also include the role of an industrial standards officer, who observes and enforces the compliance of the technical conversion of cloud services with significant technical standards. The technical management also decides on the policies of internal data handling according to requirements of the legal advisory, relevant standards and best practice.

8.3.2.3.2 Technical Revisal

The technical revisal monitors the realisation of the aforementioned policies of internal data handling. It pushes for the technical implementation of this policies as well as the adjustment to necessary changes. In case of a deviance between the policies and the actual processes the technical revisal has to intervene. The Technical revisal works closely together with the internal compliance auditing to translate its guidelines into actions.

8.3.2.3.3 Hardware maintenance

The Hardware maintenance ensures the operability of hardware components by constant attendance. This role is responsible for obviating and dealing with possible failures or breakdowns as well as exchanging, respective upgrading of parts or complete devices of machine equipment. It constantly diagnoses and repairs all hardware faults including network connections and wiring. It corresponds with the Hardware access control since the individuals who deal with the practical execution have direct access capabilities to sensitive data. Therefore, also in the context of data protection, the task of ensuring secure storage of data on reliable hardware units is a main duty. This duty must be stipulated in an internal policy, which determines the means of hardware treatment. Therefore, the Hardware maintenance works jointly together with the services of the superordinate technical management and the Technical revisal.

8.3.2.3.4 Software maintenance/updates

The Software maintenance/updates role is bound to advance the correction of software faults (maintenance) and enhancement of the general performance by the revision of the software coding (update). Part of the software maintenance is execution of software backups, firewalls, anti-malware programs (for example for the detection and removal of virus infections, Trojan horses, etc.) and diagnostic routines. It is also responsible for executing, monitoring and adjusting of security measures like e.g. anti virus programs and firewalls. The maintenance and update services mostly overlap and work jointly together with the services of the Incident management and may also be entangled with the Security management. Just like the policies imposed on the Hardware maintenance provider, the access to personal data must be restricted and controlled by the internal compliance auditing while executing the software maintenance and updates tasks.

8.3.2.3.5 Capacity/Scalability management

The capacity and/or scalability management has to monitor the performance and utilisation ratio of the available resources in order to provide dynamic on-demand resources for the customer. The monitoring enables the capacity management to satisfy the long-term requirements of the customers as well as the short term peaks of demand. Therefore, the scalability management needs to collect data on the workload of the facilities and communicate increased or decreased demands to e.g. the supplier management for further proceeding.

8.3.2.3.6 Monitoring/Metering

The monitoring observes the processes of data transferring, processing and storing within the cloud in terms of data corruption and system dysfunctions. It may also meter the demand for energy as well as the required processing capacity from the customers. If the monitoring/metering has to be considered as a data controller depends on the quality of the collected data. If the data allows inferences to be made concerning an identifiable individual the monitoring entity acts as a data controller. But even if the data only allows conclusions regarding a subscribing legal person, the information about the required capacity for example might lead e.g. to information on its economic well-being. Therefore, a noteworthy rate of the monitoring and metering data may be considered sensitive.

8.3.2.3.7 Logging

The party responsible for logging has to be differentiated from the party which is responsible for back-ups. In contrast to back-ups the log files do not provide full older versions of the data. Instead, their may be two types of log files: The event log and the access log. The event log records what is technically done to the data: e.g. when is it entered, when stored, when transferred and where but this does not yield information with regard to contents of the data. Thus, the event log might but does not necessarily contain sensitive data, which allows conclusions regarding the subscribers or end-users. The access log records who accesses the data and when. Therefore, it needs to collect information which makes the accessing person identifiable. Hence, the access log is about recording inter alia personal data of the end-users.

8.3.2.3.8 Physical security

The physical security safeguards the functional capability of all related hardware components by installing and conducting security measures regarding the physical environment. This physical security concerns the protection and surveillance of servers and other facilities as well as adequate supporting facilities such as e.g. air conditioning, heating, fire detectors. In regard to audio or video surveillance or other measures which might also monitor employees dealing with the hardware, the physical security acts as a data controller.

8.3.2.3.9 Hardware access control

The Hardware access control is closely related to the Physical security role and is designated to control the access to the hardware devices located in a specific facility to protect it from unauthorised intrusion, manipulation or destruction. The Hardware access control may be accomplished by mechanical solutions (door locks or other kind of key controls) as well as by electronic access control mechanisms, such as e.g. identification credentials to determine the authorisation of entry to the hardware facilities. This access control may not only restrict the group of persons with authorisation of access but also the manner and extent of this access. The access may also be monitored and logged in relation to the facility location and the timeframe. Because these methods of access control are also designated as personnel surveillance, they contain personal data of the hardware/facility provider's employees. Hence, the provider must be classified as data controller.

8.3.2.4 Cloud development

The development of the cloud system is a basis for the provision of cloud services as a whole. It is mandatory for the creation of the clouds system on the technical level and the embedding of new components into already existing structures. Subsequently, this can also imply the creation of successional elements which may get added to the cloud infrastructure in a later process. Therefore, these following entities that provide these services are part of the cloud provider sphere:

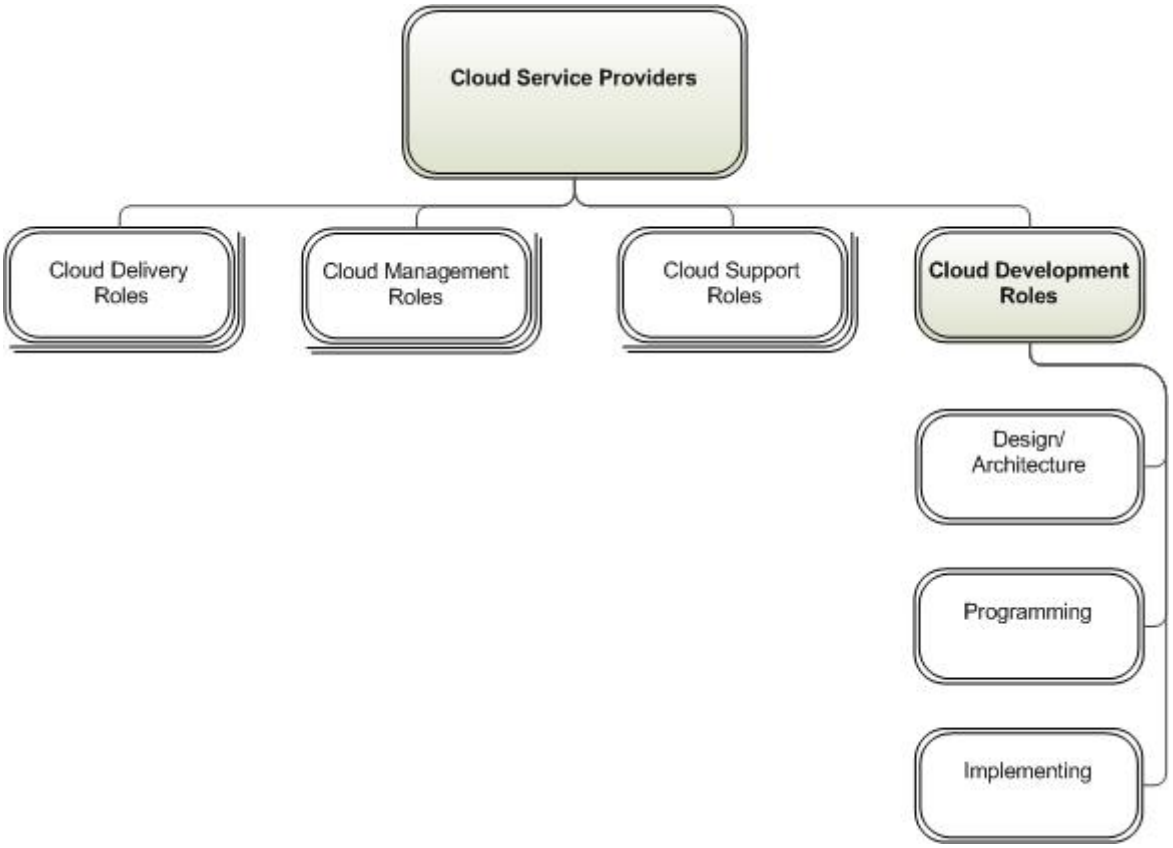


Figure 17: Cloud Development Roles

These development roles, though mostly working with not personally identifiable data might need datasets to check, control and design their programs in a test environment. If not only mock up data is used but also real (customers') data for these testing datasets, the development role might become a data controller or processer himself. Furthermore, regarding the implementation process, the responsible entity might need to access or transfer the customers' data.

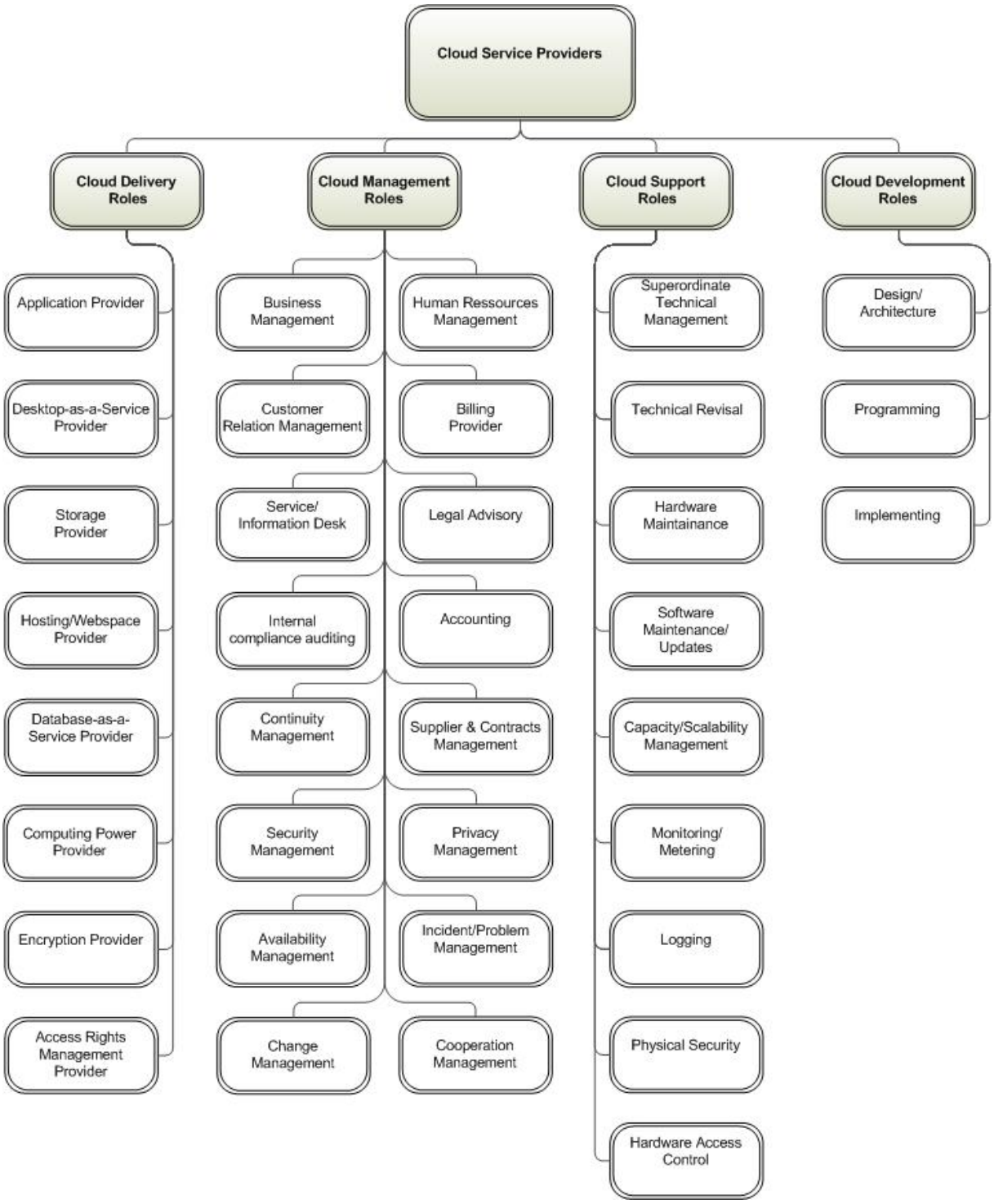


Figure 18: Overview of all Roles in the Cloud Provider Sphere

8.3.2.5 Subcontractor

The subcontractor may be contractually bound to perform part of the main contract's obligations in lieu of the cloud service provider. As the aforementioned example of salesforce.com (chap. 3) shows, subcontracting is an essential element of many cloud services. Depending on the assigned task, the subcontractor might be recipient of the subscriber's (or other data subjects') personal data. Therefore, the contracting cloud service provider has to ensure that the subcontractor is bound in the same extent in regard to this

personal data and might also have to inform his subscribers. The requirements for a notification of the subscriber depend on the assigned task as well as the location of the subcontractor, and whether the state provides an adequate level of protection for personal data in regard to the EU legal framework.

8.3.2.6 Supplier

The supplier is an external vendor of hardware, software or human resources. Depending on the contractual obligations regarding the cloud service providers and the suppliers, the latter might have a liability regarding the functionality and resilience of the provided components. There may be cases when the supplier undertakes the task of implementing hardware components himself. This opens up the possibility that the execution of this implementation gives the supplier the opportunity of getting access to data stored and processed in the cloud. Therefore, a technical as well a contractual regulation is needed to prevent the unlawful and unwanted disclosure of data towards the supplier.

8.3.2.7 Reseller

The reseller is a party that does not intend to use purchased services for himself but to resell or retail them to another party. However, this may mostly affect application services but not exclusively. The reseller may under certain circumstances have legal or contractual obligations towards the subscriber in cases of data corruption or loss caused by retailed services.

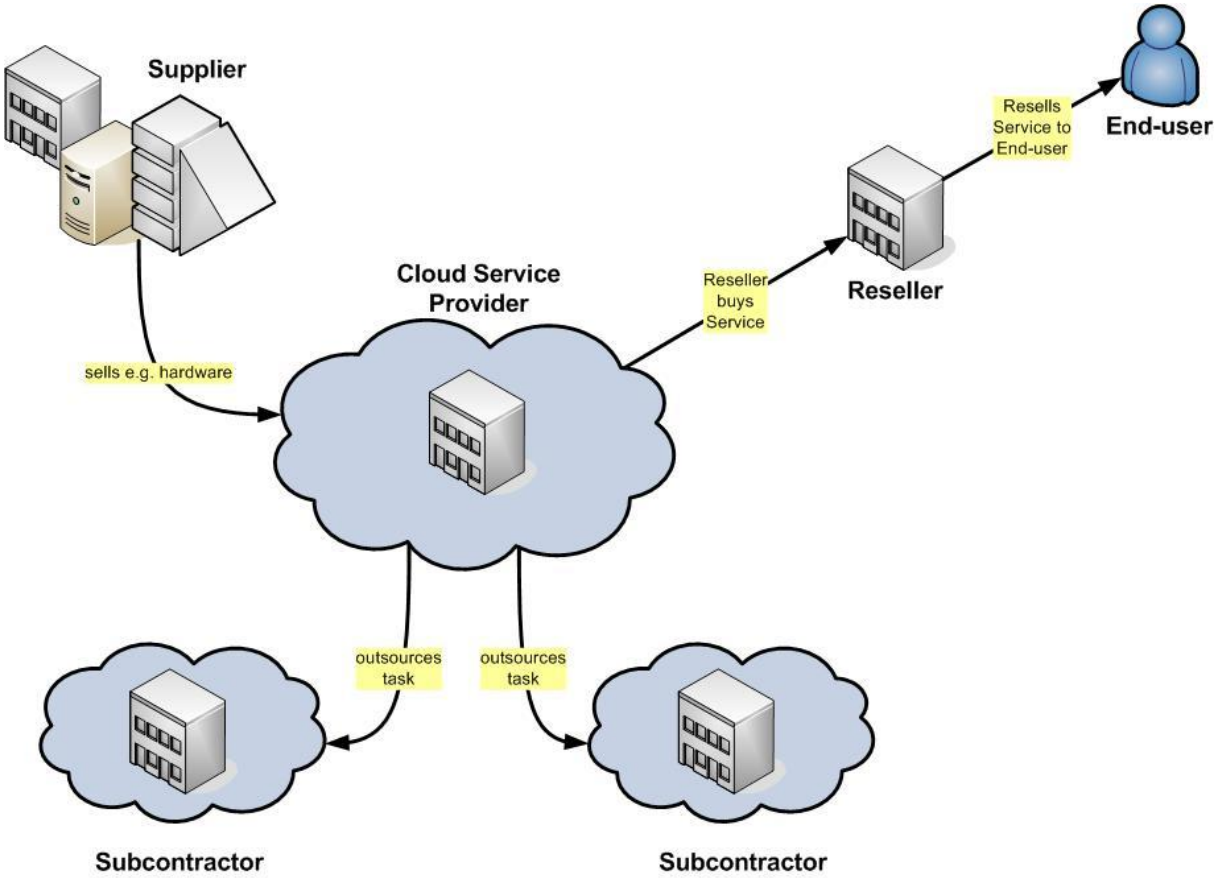


Figure 19: Roles of Subcontractor, Supplier and Reseller

8.3.3 Connection to the cloud

The connection to the cloud infrastructure is generated with the aid of the telecommunication providers and the internet access providers of the customers. Their services are not specifically cloud-related but nevertheless mandatory to claim the cloud services. These internet access or network access enablers might be able to take notice of data transferred in or out of the cloud or of end-user behaviour, if the communication is not protected. Malfunctions of these access enablers have extensive effect on the availability of cloud services. In some individual cases, a cloud broker is involved as an agent for cloud delivery services. The cloud broker may have own contractual or legal obligations related to his intermediary activity. Usually, the cloud broker has no access to data in the cloud since he only establishes the contact between the subscriber and the cloud service provider and has no direct influence or access to the mediated services on his own.

8.3.4 External influences

Aside from the above mentioned Telecommunication providers and IAP, other entities may have or desire access to cloud services and/or the data stored in a cloud infrastructure without being directly related to the subscriber or the cloud service provider sphere.

Depending on the nature of the external request against the directly cloud related parties, such external influences can be parted into different categories, for example:

1. Supervisory authorities;
2. Investigation authorities;
3. Policy makers;
4. Auditors;
5. Certification bodies;
6. Licensure authorities;
7. Other official and business entities;
8. Attackers,

All of these entities have different motivations and means to achieve access to the cloud system in some way. These motivations and means must subsequently be classified into different legal contexts. This list is by no means complete but shall give an impression of the necessity to differentiate between externals that correlate with the cloud infrastructure in some way.

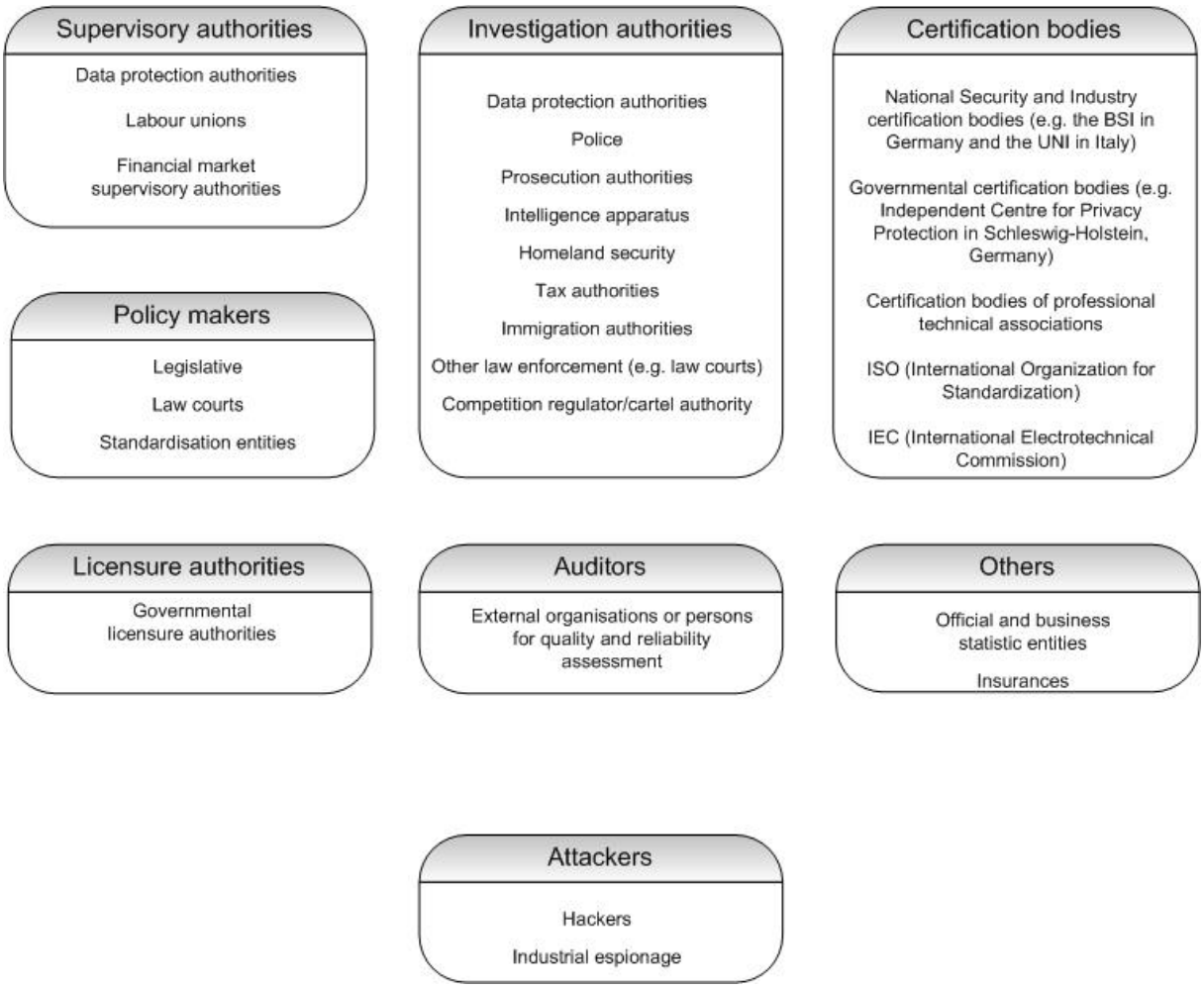


Figure 20: External Influences

8.3.4.1 Supervisory authorities

Supervisory authorities are such entities who have supervisory duties alongside controlling rights to ensure the compliance of the technical and organisational conversion of mandatory requirements. These requirements can evolve of legal frameworks as well as contractual agreements. Examples for such supervisory authorities are:

- Data protection authorities;
- Labour unions;
- Financial market supervisory authorities.

Depending on the particular law of the concerned ambit, these supervisory authorities may have a broad entitlement to access data. So many data protection authorities in the EU may have authority to inspect all documents and data which stand in close interconnection with the processing of personal data. This may include the physical access to hardware facilities and the data acquisition without the knowledge of the affected data subject. Does the data protection determine an infringement of data protection law, it may also be entitled to claim the rectification of the deficiencies and in particular serious cases may impose a sanction upon the accountable legal or natural person. Labour unions may get access to data in a cloud system in order to keep their duties regarding the privacy protection of employees. Financial market supervisory authorities may get access to data in order to monitor the activities of financial market entities. This encompasses capacious information and

disclosure obligations of the banking institutions and their vicarious agents or auxiliary persons. The financial market supervisory authorities may also have extensive authority in regard of the prevention of financial transactions with criminal background, such as money laundering and the financing of terroristic acts.

8.3.4.2 Investigation authorities

Investigation authorities are mostly governmental entities which are authorised by law to investigate in criminal cases, cases related to administrative fines, national and homeland security, tax fraud and illegal immigration. Examples for such investigation bodies are:

- Data protection authorities;
- Police;
- Prosecution authorities;
- Intelligence apparatus;
- Homeland security;
- Tax authorities;
- Immigration authorities;
- Other law enforcement (e.g. law courts);
- Competition regulator/cartel authority.

8.3.4.3 Policy makers

Policy makers are entities which phrase legally binding commitments, such as laws, directives, court decisions and obliging standards definitions. Examples for such entities are:

- Legislative;
- Law courts;
- Standardisation entities.

Apart from law courts these entities might not access data in the cloud directly, but all these policy makers are competent to state legal or technical requirements in regard to cloud services and data handling practice. Another legally binding commitment may be the use of the European standard contract clauses regarding the data processing on behalf of others. General company self-commitments outside a specific contract regarding not mandatory industrial standards may also be the work of policy makers once they achieve a stringent obligation of the conducting company. Besides the fixation of technical standards, such a self-commitment can also be of a more legal or functional nature and may be laid down in official Binding Corporate Rules (BCR).

8.3.4.4 Auditors

Auditors refer to the external organisations or persons, who ascertain the quality and reliability of a specific service or process. They might also provide an assessment of a system's internal control. Auditors get granular on the inspected process and evaluate it on the basis of technical and/or legal requirements. The outcome is the auditor's opinion on the compliance to the predetermined requirements. The audit may be essential for the service provider to prove the conformance of their offered services with their contractual, legal and technical obligations. This may open up the possibility for the customer to verify the adherence of the provider's activities with his policies. It may also function as evidence concerning the elimination of former problem areas and a management tool for achieving

continual improvement in the organisation. The passing of the audit may also gain the provider a better market position by becoming more attractive for potential customers. In most cases, the auditor cannot ascertain if the affected party has provided all the necessary information without hiding possible faults regarding a reviewed process. Therefore, the auditor generally precludes any liability in regard of his opinion. Furthermore, the audit refers only to the specific date of the inspection; later changes might have led to another outcome. Certification bodies may rely on the auditor's opinion as a basis for their certification decision.

8.3.4.5 Certification bodies

Certification bodies are intended to assess a company in regard to the quality of hardware, software and data processing procedures. The relevant frame condition is the compliance of the company's products and services with mandatory legal and technical requirements. These Certification bodies also assess the qualification of the company's personnel related to a certain product version. In the IT and software engineering industry, the proven professionalism enables employed individuals to hold specific positions in this particular field. Nevertheless, this certification may only be valid for a specific version of the product or must be renewed in certain time intervals. Usually, the review of an auditor is basis for the certification. Examples for official and recognised certification bodies which have established standards which may be relevant in regard to cloud computing are:

- National Security and Industry certification bodies (e.g. the BSI in Germany and the UNI in Italy);
- Governmental certification bodies (e.g. Independent Centre for Privacy Protection in Schleswig-Holstein, Germany);
- Certification bodies of professional technical associations, for example of:
  - the German TÜV (Technischer Überwachungs-Verein);
  - the ENEC (European Norms Electrical Certification);
  - the GEC (Green Electronics Council);
- ISO (International Organization for Standardization);
- IEC (International Electrotechnical Commission).

8.3.4.6 Licensure authorities

Licensure authorities give the permission to practise in a specific occupational area. Governmental authorities license certain activities to regulate areas which are deemed to involve a high level of skill or specialisation. Therefore, licensing should prevent people from getting harmed by a layperson. E.g. in the medical sector many states restrict the permission to practice medicine or to deal with medical data to persons with a medical license bestowed either by a specified government-approved professional association or a government agency. Therefore, in case of cloud computing either the subscriber or - dependent on the contracts - the provider may have to ensure that certain data is only accessed by officially licensed persons.

8.3.4.7 Other official and business entities

Other official and business entities may have access to data stored and processed in the cloud to meet their specific functions and purposes. Such entities are for example statistics entities and insurances. Exemplary, statistic entities may desire access to enumerative data to determine parameters to be used in surveys, probability studies and publications. There is a various number of fields to which this enumerative data may belong, such as e.g. demography, econometrics, geostatistics and actuarial science. In Europe, statistic

authorities have extensive authorisation to collect data e.g. regarding a company's employees, their age, profession and salary. This may affect the cloud service provider as well as a subscribing company, which processes its human resources data in the cloud. Just like financial market supervisory authorities, insurances may also claim data stored and processed in the cloud to fulfil legally stated duties of preventing criminally motivated financial transactions. Insurances also may be entitled to collect data for statistic purposes, such as actuarial science to assess insurance risks.

8.3.4.8 Attackers

Another external influence with an effect to cloud infrastructures are attackers. The attacker breaks into a cloud system to gain unauthorised access to services and data. He may use various techniques and mechanisms to overpower security and privacy protection instalments, such as man-in-the-middle attacks, wiretapping, spoofing, phishing, Trojan horses, viruses, worms, key-loggers, social engineering and password-cracking. The motivation of the attackers may be of monetary interests, vandalism or other incentives. Nevertheless, in many cases a relevant motivation may be industrial espionage to learn of company-internal knowledge with potential market value. Other attack intentions may e.g. be credit card frauds, identity theft, blackmailing and malicious injury of property.

8.4 Exemplary role model: Conclusion and supplementary considerations

This exemplary role is designated to convey a common understanding of the different entities that may be involved within a cloud computing setting. The comprised roles thereby present a general infrastructural overview of various possible cloud service scenarios to approach critical legal issues evolving around the cloud computing field in general. This role model, however, does not embody ready solutions for the allocation of legal responsibilities. Rather, it is a first indispensable step to make such allocation possible subsequently. Thus, for the final determination of data protection-wise obligations and their corresponding legal responsibilities, it is mandatory to do a precisely analysis of the factual actions taken by the individual parties. This enables an appropriate classification of these parties as data controllers or data processors, depending on their influence on the collection, storage and processing of personal data. Only once the hurdle of such classification has been mastered, the legal consequences can be correctly determined and conclusions can be drawn.

Chapter 9

Basic terminology and concepts (Annex B)

Below are several terms in alphabetical order that were used in the main document and Annex A. These definitions were created with reference to the frameworks of the EU Data Protection Directive 95/46/EC and the EU E-Privacy Directive 2002/58/EC including its amending Directive 2009/136/EC. Furthermore, the definitions of the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, adopted on 23 September 1980, in its respective latest version, were taken into account.

Anonymisation

“Rendering anonymous” shall mean the alteration of personal data so the comprised information cannot be referenced to an identified or identifiable natural person. Technically, anonymity of a subject means that the subject can not be uniquely characterised within a set of all possible subjects, the anonymity set[309] (See also the difference to pseudonymisation).

Collection of personal data

“Data Collection” (“collecting”) is the acquisition of personal data on the data subject for processing.

Contractual data

"Contractual data" is data, which must be collected and processed to enable the conclusion, contextual constitution, alteration and termination of a contract between the provider and the user. These may be for example the name and invoice address and of the user.

Customer

The “customer” is a natural person, a corporate entity or a municipality who purchases the IT-services offered by the CSP.

Data subject

The “data subject” is an individual whose personal data is collected in a way that makes the individual theoretically identifiable.

End-user

The term "end-user" must be differed from the terms "customer", "dependent end-user" and "data subject". An "end-user" is a natural person [E-Privacy Directive 2002/58/EC Article 2

[309] Pfitzmann/Hansen, *A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management*, p. 9.

(a)] who uses the cloud application front end to use, process and store the data (not necessarily his own), e.g. employees of the data controller and maybe the data subject himself. The term "dependent end-user" shall mean an end-user, who may have access to the data but who is not authorised to make crucial decisions regarding the data such as data access management and the means of the data processing and storing.

IaaS – Infrastructure as a Service

“Infrastructure as a Service (IaaS)” is the provision of fundamental computing resources, e.g. computing, storage, networking, systems- and network-management where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications.

Informed consent of the data subject

The data subject's "informed consent" shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed [EU Directive 95/46/EC Article 2(h)]. It is necessary that the data subject is aware of the extent and modality of the data processing.

Internet Access Provider (IAP)

An Internet Access Provider (IAP) is a company that offers its customers access to the internet. In this context, the term IAP is equivalent to the commonly used term Internet Service Provider (ISP).

Multi-tenancy

"Multi-tenancy" means the sharing of resources across a large pool of customers and/or users by measures that enable each user to only access and process his own data without interfering with other users.

PaaS – Platform as a Service

“Platform as a Service (PaaS)” offers the customer a runtime computing or development environment which can e.g. be used for developing and executing applications within this platform. The platform facilitates the deployment of acquired applications created by the customer using programming languages and tools supported by the provider. The vendor of PaaS often also provides other services such as IaaS or application hosting.

Personal data

"Data" is generally abstract information which defines a single or several attributes in a set of variables. "Personal data" shall mean any information relating to an identified or identifiable individual (data subject) [see EU Directive 95/46/EC Article 2(a)]. Identifiability is given if the information conveys a direct or indirect connection to a particular physical person. Such information could be for example a civil registration number or an email address that could be linked to the data subject [OECD Guidelines Section B Detailed Comments, paragraph 41]. Even statistic data might be personal data if the target group is small enough to relate information to a specific person of this group. Data which conveys information about race, ethnicity, political opinion, religion or philosophical beliefs, health or sex life of an individual is usually considered as personal data with a high level of sensitivity.

Processing of personal data

“Processing of personal data” (“processing”) shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction (EU Data Protection Directive Article 2 (b)).

Pseudonymisation

"Pseudonymisation" or "aliasing" means the replacement of the data subject’s name and other name-related features with a dissimilar identifier to preclude or hinder the identification of the data subject. In contrast to anonymisation the data is still related to a specific identifier.[310]

Purpose

The EU Data Protection Directive 95/46/EC states in Article 28, that the collection and processing of data must be predetermined for a specific purpose. Generally, a purpose is the main goal or motivation of an activity or behaviour. In the context of the EU directive, this means the purpose of the data processing must coincide with the purpose for which the data was originally collected. This applies especially for particular sensitive data, such as health-related data. Nevertheless, there are some exceptions and also restrictions to this general regulation. So for example, under certain circumstances some latitude is given for a further data processing for historical, statistical or scientific purposes as far as it is not evidently incompatible with the original purpose of the data collection. Furthermore, under certain circumstances related to the European Convention’s most fundamental guarantees of Human Rights and Freedoms, purposes of journalistic, literary or artistic expressions also qualify for some exclusion of the predetermination. Also, legal obligations of professional secrecy facilitate a derogation from the predetermination (see EU Data Protection Directive 95/46/EC recitals (28), (29), (33), (37)).

Recipient

A "recipient" is a natural or legal person to whom or which data is disclosed [see EU Directive 95/46/EC Article 2 (g)].

Recording of data

“Data recording” (“recording”) shall mean the input, recording and/or preservation of personal data on a storage medium for further processing or usage.

SaaS – Software as a Service

Cloud application services or “Software as a Service (SaaS)” deliver the access to a specific software application over the Internet. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based e-mail). SaaS often is comprised of several provided services e.g. storage in conjunction with the cloud application. SaaS is often based upon other services, such as the underlying platform and infrastructure that go along with the provided software application.

[310] Cf. Pfitzmann/Hansen, p. 21.

Terminal equipment/user devices

Terminal equipment or user devices shall mean the user's electronic equipment to access and use electronic communication networks (e.g. mobile phone, personal computer).

Traffic data

"Traffic data" is any data which must be collected and processed to enable the usage of an electronic communication network or the billing thereof. Traffic data may consist of data referring to the routing, time and amount of the communication, the protocols used, the data format the location of the terminal equipment and to the duration and degree of the accessed cloud services (for pay-as-you-go-billing). In the case of cloud computing, the application provider also needs to collect e.g. information about the terminal equipment the user deploys to access the application. The reason for this collecting of personal data is that the display of the application front end may differ dependent on whether the user resorts to a mobile phone, a personal computer or another terminal device [E-Privacy Directive 2002/58/EC Article 2 (b) and 2009/139/EC recital (53)] .

Chapter 10

Safe Harbor FAQ (Annex C)

10.1 FAQ Sensitive Data

Must an organization always provide explicit (opt in) choice with respect to sensitive data?

No, such choice is not required where the processing is:

(1) in the vital interests of the data subject or another person;

(2) necessary for the establishment of legal claims or defenses;

(3) required to provide medical care or diagnosis;

(4) carried out in the course of legitimate activities by a foundation, association or any other non-profit body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members of the body or to the persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects;

(5) necessary to carry out the organization's obligations in the field of employment law; or

(6) related to data that are manifestly made public by the individual.[311]

10.2 FAQ Journalistic Exceptions

Given U.S. constitutional protections for freedom of the press and the Directive's exemption for journalistic material, do the Safe Harbor Principles apply to personal information gathered, maintained, or disseminated for journalistic purposes?

Where the rights of a free press embodied in the First Amendment of the U.S. Constitution intersect with privacy protection interests, the First Amendment must govern the balancing of these interests with regard to the activities of U.S. persons or organizations. Personal information that is gathered for publication, broadcast, or other forms of public communication of journalistic material, whether used or not, as well as information found in previously published material disseminated from media archives, is not subject to the requirements of the Safe Harbor Principles.[312]

10.3 FAQ Secondary Liability

Are Internet service providers (ISPs), telecommunications carriers, or other organizations liable under the Safe Harbor Principles when on behalf of another organization they merely transmit, route, switch or cache information that may violate their terms?

---

[311] http://www.export.gov/safeharbor/eu/eg_main_018375.asp .

[312] http://www.export.gov/safeharbor/eu/eg_main_018367.asp .

No. As is the case with the Directive itself, the safe harbor does not create secondary liability. To the extent that an organization is acting as a mere conduit for data transmitted by third parties and does not determine the purposes and means of processing those personal data, it would not be liable.[313]

10.4 FAQ Investment banking and audits

The activities of auditors and investment bankers may involve processing personal data without the consent or knowledge of the individual. Under what circumstances is this permitted by the Notice, Choice, and Access Principles?

Investment bankers or auditors may process information without knowledge of the individual only to the extent and for the period necessary to meet statutory or public interest requirements and in other circumstances in which the application of these Principles would prejudice the legitimate interests of the organization. These legitimate interests include the monitoring of companies' compliance with their legal obligations and legitimate accounting activities, and the need for confidentiality connected with possible acquisitions, mergers, joint ventures, or other similar transactions carried out by investment bankers or auditors.[314]

10.5 FAQ The Role of the Data Protection Authorities

How will companies that commit to cooperate with European Union Data Protection Authorities (DPAs) make those commitments and how will they be implemented?

Under the safe harbor, U.S. organizations receiving personal data from the EU must commit to employ effective mechanisms for assuring compliance with the Safe Harbor Principles. More specifically as set out in the Enforcement Principle, they must provide (a) recourse for individuals to whom the data relate, (b) follow up procedures for verifying that the attestations and assertions they have made about their privacy practices are true, and (c) obligations to remedy problems arising out of failure to comply with the Principles and consequences for such organizations. An organization may satisfy points (a) and (c) of the Enforcement Principle if it adheres to the requirements of this FAQ for cooperating with the DPAs.

An organization may commit to cooperate with the DPAs by declaring in its safe harbor certification to the Department of Commerce (see FAQ on self-certification) that the organization:

1. elects to satisfy the requirement in points (a) and (c) of the Safe Harbor Enforcement Principle by committing to cooperate with the DPAs;

2. will cooperate with the DPAs in the investigation and resolution of complaints brought under the safe harbor; and

3. will comply with any advice given by the DPAs where the DPAs take the view that the organization needs to take specific action to comply with the Safe Harbor Principles, including remedial or compensatory measures for the benefit of individuals affected by any non-compliance with the Principles, and will provide the DPAs with written confirmation that such action has been taken.

[313] http://www.export.gov/safeharbor/eu/eg_main_018376.asp .

[314] http://www.export.gov/safeharbor/eu/eg_main_018377.asp .

The cooperation of the DPAs will be provided in the form of information and advice in the following way:

The advice of the DPAs will be delivered through an informal panel of DPAs established at the European Union level, which will inter alia help ensure a harmonised and coherent approach.

The panel will provide advice to the U.S. organizations concerned on unresolved complaints from individuals about the handling of personal information that has been transferred from the EU under the safe harbor. This advice will be designed to ensure that the Safe Harbor Principles are being correctly applied and will include any remedies for the individual(s) concerned that the DPAs consider appropriate.

The panel will provide such advice in response to referrals from the organizations concerned and/or to complaints received directly from individuals against organizations which have committed to cooperate with DPAs for safe harbor purposes, while encouraging and if necessary helping such individuals in the first instance to use the in-house complaint handling arrangements that the organization may offer.

Advice will be issued only after both sides in a dispute have had a reasonable opportunity to comment and to provide any evidence they wish. The panel will seek to deliver advice as quickly as this requirement for due process allows. As a general rule, the panel will aim to provide advice within 60 days after receiving a complaint or referral and more quickly where possible.

The panel will make public the results of its consideration of complaints submitted to it, if it sees fit.

The delivery of advice through the panel will not give rise to any liability for the panel or for individual DPAs.

As noted above, organizations choosing this option for dispute resolution must undertake to comply with the advice of the DPAs. If an organization fails to comply within 25 days of the delivery of the advice and has offered no satisfactory explanation for the delay, the panel will give notice of its intention either to submit the matter to the Federal Trade Commission or other U.S. federal or state body with statutory powers to take enforcement action in cases of deception or misrepresentation, or to conclude that the agreement to cooperate has been seriously breached and must therefore be considered null and void. In the latter case, the panel will inform the Department of Commerce (or its designee) so that the list of safe harbor participants can be duly amended. Any failure to fulfill the undertaking to cooperate with the DPAs, as well as failures to comply with the Safe Harbor Principles, will be actionable as a deceptive practice under Section 5 of the FTC Act or other similar statute.

Organizations choosing this option will be required to pay an annual fee which will be designed to cover the operating costs of the panel, and they may additionally be asked to meet any necessary translation expenses arising out of the panel's consideration of referrals or complaints against them. The annual fee will not exceed $500 and will be less for smaller companies.

The option of co-operating with the DPAs will be available to organizations joining the safe harbor during a three-year period. The DPAs will reconsider this arrangement before the end of that period if the number of U.S. organizations choosing this option proves to be excessive.[315]

[315] http://www.export.gov/safeharbor/eu/eg_main_018378.asp .

10.6 FAQ Self-Certification

How does an organization self-certify that it adheres to the Safe Harbor Principles?

Safe harbor benefits are assured from the date on which an organization self-certifies to the Department of Commerce (or its designee) its adherence to the Principles in accordance with the guidance set forth below.

To self-certify for the safe harbor, organizations can provide to the Department of Commerce (or its designee) a letter, signed by a corporate officer on behalf of the organization that is joining the safe harbor, that contains at least the following information:

1. name of organization, mailing address, email address, telephone and fax numbers;

2. description of the activities of the organization with respect to personal information received from the EU; and

3. description of the organization's privacy policy for such personal information, including:

a. where the privacy policy is available for viewing by the public,

b. its effective date of implementation,

c. a contact office for the handling of complaints, access requests, and any other issues arising under the safe harbor,

d. the specific statutory body that has jurisdiction to hear any claims against the organization regarding possible unfair or deceptive practices and violations of laws or regulations governing privacy (and that is listed in the annex to the Principles),

e. name of any privacy programs in which the organization is a member,

f. method of verification (e.g. in-house, third party) [see FAQ Verification], and

g. the independent recourse mechanism that is available to investigate unresolved complaints.

Where the organization wishes its safe harbor benefits to cover human resources information transferred from the EU for use in the context of the employment relationship, it may do so where there is a statutory body with jurisdiction to hear claims against the organization arising out of human resources information that is listed in the annex to the Principles. In addition the organization must indicate this in its letter and declare its commitment to cooperate with the EU authority or authorities concerned in conformity with FAQ – Human resources and FAQ – Data Protection as applicable and that it will comply with the advice given by such authorities.

The Department (or its designee) will maintain a list of all organizations that file such letters, thereby assuring the availability of safe harbor benefits, and will update such list on the basis of annual letters and notifications received pursuant to FAQ – Dispute Resolution. Such self-certification letters should be provided not less than annually. Otherwise the organization will be removed from the list and safe harbor benefits will no longer be assured. Both the list and the self-certification letters submitted by the organizations will be made publicly available. All organizations that self- certify for the safe harbor must also state in their relevant published privacy policy statements that they adhere to the Safe Harbor Principles.

The undertaking to adhere to the Safe Harbor Principles is not time-limited in respect of data received during the period in which the organization enjoys the benefits of the safe harbor. Its undertaking means that it will continue to apply the Principles to such data for as long as the organization stores, uses or discloses them, even if it subsequently leaves the safe harbor for any reason.

An organization that will cease to exist as a separate legal entity as a result of a merger or a takeover must notify the Department of Commerce (or its designee) of this in advance. The

notification should also indicate whether the acquiring entity or the entity resulting from the merger will (1) continue to be bound by the Safe Harbor Principles by the operation of law governing the takeover or merger or (2) elect to self-certify its adherence to the Safe Harbor Principles or put in place other safeguards, such as a written agreement that will ensure adherence to the Safe Harbor Principles. Where neither (1) nor (2) applies, any data that has been acquired under the safe harbor must be promptly deleted.

An organization does not need to subject all personal information to the Safe Harbor Principles, but it must subject to the Safe Harbor Principles all personal data received from the EU after it joins the safe harbor.

Any misrepresentation to the general public concerning an organization's adherence to the Safe Harbor Principles may be actionable by the Federal Trade Commission or other relevant government body. Misrepresentations to the Department of Commerce (or its designee) may be actionable under the False Statements Act (18 U.S.C. § 1001).[316]

10.7 FAQ Verification

How do organizations provide follow up procedures for verifying that the attestations and assertions they make about their safe harbor privacy practices are true and those privacy practices have been implemented as represented and in accordance with the Safe Harbor Principles?

To meet the verification requirements of the Enforcement Principle, an organization may verify such attestations and assertions either through self-assessment or outside compliance reviews.

Under the self- assessment approach, such verification would have to indicate that an organization's published privacy policy regarding personal information received from the EU is accurate, comprehensive, prominently displayed, completely implemented and accessible. It would also need to indicate that its privacy policy conforms to the Safe Harbor Principles; that individuals are informed of any in-house arrangements for handling complaints and of the independent mechanisms through which they may pursue complaints; that it has in place procedures for training employees in its implementation, and disciplining them for failure to follow it; and that it has in place internal procedures for periodically conducting objective reviews of compliance with the above. A statement verifying the self- assessment should be signed by a corporate officer or other authorized representative of the organization at least once a year and made available upon request by individuals or in the context of an investigation or a complaint about non-compliance.

Organizations should retain their records on the implementation of their safe harbor privacy practices and make them available upon request in the context of an investigation or a complaint about non-compliance to the independent body responsible for investigating complaints or to the agency with unfair and deceptive practices jurisdiction.

Where the organization has chosen outside compliance review, such a review needs to demonstrate that its privacy policy regarding personal information received from the EU conforms to the Safe Harbor Principles that it is being complied with and that individuals are informed of the mechanisms through which they may pursue complaints. The methods of review may include without limitation auditing, random reviews, use of "decoys," or use of technology tools as appropriate. A statement verifying that an outside compliance review has been successfully completed should be signed either by the reviewer or by the corporate officer or other authorized representative of the organization at least once a year and made

[316] http://www.export.gov/safeharbor/eu/eg_main_018388.asp .

available upon request by individuals or in the context of an investigation or a complaint about compliance.[317]

10.8 FAQ Access

Individuals must have access to personal information about them that an organization holds and be able to correct, amend or delete that information where it is inaccurate, except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question, or where the legitimate rights of persons other than the individual would be violated.

1. Is the right of access absolute?

No. Under the Safe Harbor Principles, the right of access is fundamental to privacy protection. In particular, it allows individuals to verify the accuracy of information held about them. Nonetheless, the obligation of an organization to provide access to the personal information it holds about an individual is subject to the principle of proportionality or reasonableness and has to be tempered in certain instances. Indeed, the Explanatory Memorandum to the 1980 OECD Privacy Guidelines makes clear that an organization's access obligation is not absolute. It does not require the exceedingly thorough search mandated, for example, by a subpoena, nor does it require access to all the different forms in which the information may be maintained by the organization.

Rather, experience has shown that in responding to individuals' access requests, organizations should first be guided by the concern(s) that led to the requests in the first place. For example, if an access request is vague or broad in scope, an organization may engage the individual in a dialogue so as to better understand the motivation for the request and to locate responsive information. The organization might inquire about which part(s) of the organization the individual interacted with and/or about the nature of the information (or its use) that is the subject of the access request. Individuals do not, however, have to justify requests for access to their own data.

Expense and burden are important factors and should be taken into account but they are not controlling in determining whether providing access is reasonable. For example, if the information is used for decisions that will significantly affect the individual (e.g., the denial or grant of important benefits, such as insurance, a mortgage, or a job), then consistent with the other provisions of these FAQs, the organization would have to disclose that information even if it is relatively difficult or expensive to provide.

If the information requested is not sensitive or not used for decisions that will significantly affect the individual (e.g., non-sensitive marketing data that is used to determine whether or not to send the individual a catalog), but is readily available and inexpensive to provide, an organization would have to provide access to factual information that the organization stores about the individual. The information concerned could include facts obtained from the individual, facts gathered in the course of a transaction, or facts obtained from others that pertain to the individual.

Consistent with the fundamental nature of access, organizations should always make good faith efforts to provide access. For example, where certain information needs to be protected and can be readily separated from other information subject to an access request, the organization should redact the protected information and make available the other information. If an organization determines that access should be denied in any particular

[317] http://www.export.gov/safeharbor/eu/eg_main_018379.asp .

instance, it should provide the individual requesting access with an explanation of why it has made that determination and a contact point for any further inquiries.

2. What is confidential commercial information and may organizations deny access in order to safeguard it?

Confidential commercial information (as that term is used in the Federal Rules of Civil Procedure on discovery) is information which an organization has taken steps to protect from disclosure, where disclosure would help a competitor in the market. The particular computer program an organization uses, such as a modeling program, or the details of that program may be confidential commercial information. Where confidential commercial information can be readily separated from other information subject to an access request, the organization should redact the confidential commercial information and make available the non-confidential information. Organizations may deny or limit access to the extent that granting it would reveal its own confidential commercial information as defined above, such as marketing inferences or classifications generated by the organization, or the confidential commercial information of another where such information is subject to a contractual obligation of confidentiality in circumstances where such an obligation of confidentiality would normally be undertaken or imposed.

3. In providing access, may an organization disclose to individuals personal information about them derived from its data bases or is access to the data base itself required?

Access can be provided in the form of disclosure by an organization to the individual and does not require access by the individual to an organization's data base.

4. Does an organization have to restructure its data bases to be able to provide access?

Access needs to be provided only to the extent that an organization stores the information. The access principle does not itself create any obligation to retain, maintain, reorganize, or restructure personal information files.

5. These replies make clear that access may be denied in certain circumstances. In what other circumstances may an organization deny individuals access to their personal information?

Such circumstances are limited, and any reasons for denying access must be specific. An organization can refuse to provide access to information to the extent that disclosure is likely to interfere with the safeguarding of important countervailing public interests, such as national security; defense; or public security. In addition, where personal information is processed solely for research or statistical purposes, access may be denied. Other reasons for denying or limiting access are:

- *a. interference with execution or enforcement of the law, including the prevention, investigation or detection of offenses or the right to a fair trial;*
- *b. interference with private causes of action, including the prevention, investigation or detection of legal claims or the right to a fair trial;*
- *c. disclosure of personal information pertaining to other individual(s) where such references cannot be redacted;*
- *d. breaching a legal or other professional privilege or obligation;*

e. breaching the necessary confidentiality of future or ongoing negotiations, such as those involving the acquisition of publicly quoted companies;

f. prejudicing employee security investigations or grievance proceedings;

g. prejudicing the confidentiality that may be necessary for limited periods in connection with employee succession planning and corporate re-organizations; or

h. prejudicing the confidentiality that may be necessary in connection with monitoring, inspection or regulatory functions connected with sound economic or financial management; or

i. other circumstances in which the burden or cost of providing access would be disproportionate or the legitimate rights or interests of others would be violated.

An organization which claims an exception has the burden of demonstrating its applicability (as is normally the case). As noted above, the reasons for denying or limiting access and a contact point for further inquiries should be given to individuals.

6. Can an organization charge a fee to cover the cost of providing access?

Yes. The OECD Guidelines recognize that organizations may charge a fee, provided that it is not excessive. Thus organizations may charge a reasonable fee for access. Charging a fee may be useful in discouraging repetitive and vexatious requests.

Organizations that are in the business of selling publicly available information may thus charge the organization's customary fee in responding to requests for access. Individuals may alternatively seek access to their information from the organization that originally compiled the data.

Access may not be refused on cost grounds if the individual offers to pay the costs.

7. Is an organization required to provide access to personal information derived from public records?

To clarify first, public records are those records kept by government agencies or entities at any level that are open to consultation by the public in general. It is not necessary to apply the Access Principle to such information as long as it is not combined with other personal information, apart from when small amounts of non-public record information are used for indexing or organizing public record information. However, any conditions for consultation established by the relevant jurisdiction are to be respected. Where public record information is combined with other non-public record information (other than as specifically noted above), however, an organization must provide access to all such information, assuming it is not subject to other permitted exceptions.

8. Does the Access Principle have to be applied to publicly available personal information?

As with public record information (see Q7), it is not necessary to provide access to information that is already publicly available to the public at large, as long as it is not combined with non-publicly available information.

9. How can an organization protect itself against repetitious or vexatious requests for access?

An organization does not have to respond to such requests for access. For these reasons, organizations may charge a reasonable fee and may set reasonable limits on the number of

times within a given period that access requests from a particular individual will be met. In setting such limitations, an organization should consider such factors as the frequency with which information is updated, the purpose for which the data are used, and the nature of the information.

10. How can an organization protect itself against fraudulent requests for access?

An organization is not required to provide access unless it is supplied with sufficient information to allow it to confirm the identity of the person making the request.

11. Is there a time within which responses must be provided to access requests?

Yes, organizations should respond without excessive delay and within a reasonable time period. This requirement may be satisfied in different ways as the explanatory memorandum to the 1980 OECD Privacy Guidelines states. For example, a data controller who provides information to data subjects at regular intervals may be exempted from obligations to respond at once to individual requests.[318]

10.9 FAQ Human Resources

1. Is the transfer from the EU to the United States of personal information collected in the context of the employment relationship covered by the safe harbor?

Yes, where a company in the EU transfers personal information about its employees (past or present) collected in the context of the employment relationship, to a parent, affiliate, or unaffiliated service provider in the United States participating in the safe harbor, the transfer enjoys the benefits of the safe harbor. In such cases, the collection of the information and its processing prior to transfer will have been subject to the national laws of the EU country where it was collected, and any conditions for or restrictions on its transfer according to those laws will have to be respected.

The Safe Harbor Principles are relevant only when individually identified records are transferred or accessed. Statistical reporting relying on aggregate employment data and/or the use of anonymized or pseudonymized data does not raise privacy concerns.

2. How do the Notice and Choice Principles apply to such information?

A U.S. organization that has received employee information from the EU under the safe harbor may disclose it to third parties and/or use it for different purposes only in accordance with the Notice and Choice Principles. For example, where an organization intends to use personal information collected through the employment relationship for non-employment-related purposes, such as marketing communications, the U.S. organization must provide the affected individuals with choice before doing so, unless they have already authorized the use of the information for such purposes. Moreover, such choices must not be used to restrict employment opportunities or take any punitive action against such employees.

It should be noted that certain generally applicable conditions for transfer from some Member States may preclude other uses of such information even after transfer outside the EU and such conditions will have to be respected.

[318] http://www.export.gov/safeharbor/eu/eg_main_018380.asp .

In addition, employers should make reasonable efforts to accommodate employee privacy preferences. This could include, for example, restricting access to the data, anonymizing certain data, or assigning codes or pseudonyms when the actual names are not required for the management purpose at hand.

To the extent and for the period necessary to avoid prejudicing the legitimate interests of the organization in making promotions, appointments, or other similar employment decisions, an organization does not need to offer notice and choice.

3. How does the Access Principle apply?

The FAQs on access provide guidance on reasons which may justify denying or limiting access on request in the human resources context. Of course, employers in the European Union must comply with local regulations and ensure that European Union employees have access to such information as is required by law in their home countries, regardless of the location of data processing and storage. The safe harbor requires that an organization processing such data in the United States will cooperate in providing such access either directly or through the EU employer.

4. How will enforcement be handled for employee data under the Safe Harbor Principles?

In so far as information is used only in the context of the employment relationship, primary responsibility for the data vis-à-vis the employee remains with the company in the EU. It follows that, where European employees make complaints about violations of their data protection rights and are not satisfied with the results of internal review, complaint, and appeal procedures (or any applicable grievance procedures under a contract with a trade union), they should be directed to the state or national data protection or labor authority in the jurisdiction where the employee works. This also includes cases where the alleged mishandling of their personal information has taken place in the United States, is the responsibility of the U.S. organization that has received the information from the employer and not of the employer and thus involves an alleged breach of the Safe Harbor Principles, rather than of national laws implementing the Directive. This will be the most efficient way to address the often overlapping rights and obligations imposed by local labor law and labor agreements as well as data protection law.

A U.S. organization participating in the safe harbor that uses EU human resources data transferred from the Europe Union in the context of the employment relationship and that wishes such transfers to be covered by the safe harbor must therefore commit to cooperate in investigations by and to comply with the advice of competent EU authorities in such cases. The DPAs that have agreed to cooperate in this way will notify the European Commission and the Department of Commerce. If a U.S. organization participating in the safe harbor wishes to transfer human resources data from a Member State where the DPA has not so agreed, the provisions of FAQ – Data Protection will apply.[319]

10.10 FAQ Contracts

When data is transferred from the EU to the United States only for processing purposes, will a contract be required, regardless of participation by the processor in the safe harbor?

[319] http://www.export.gov/safeharbor/eu/eg_main_018381.asp .

Yes. Data controllers in the European Union are always required to enter into a contract when a transfer for mere processing is made, whether the processing operation is carried out inside or outside the EU. The purpose of the contract is to protect the interests of the data controller, i.e. the person or body who determines the purposes and means of processing, who retains full responsibility for the data vis-à-vis the individual(s) concerned. The contract thus specifies the processing to be carried out and any measures necessary to ensure that the data are kept secure.

A U.S. organization participating in the safe harbor and receiving personal information from the EU merely for processing thus does not have to apply the Principles to this information, because the controller in the EU remains responsible for it vis-à-vis the individual in accordance with the relevant EU provisions (which may be more stringent than the equivalent Safe Harbor Principles).

Because adequate protection is provided by safe harbor participants, contracts with safe harbor participants for mere processing do not require prior authorization (or such authorization will be granted automatically by the Member States) as would be required for contracts with recipients not participating in the safe harbor or otherwise not providing adequate protection.[320]

10.11 FAQ Dispute Resolution and Enforcement

How should the dispute resolution requirements of the Enforcement Principle be implemented, and how will an organization's persistent failure to comply with the Principles be handled?

The Enforcement Principle sets out the requirements for safe harbor enforcement. How to meet the requirements of point (b) of the Principle is set out in the FAQ on verification. This FAQ addresses points (a) and (c), both of which require independent recourse mechanisms. These mechanisms may take different forms, but they must meet the Enforcement Principle's requirements. Organizations may satisfy the requirements through the following: (1) compliance with private sector developed privacy programs that incorporate the Safe Harbor Principles into their rules and that include effective enforcement mechanisms of the type described in the Enforcement Principle; (2) compliance with legal or regulatory supervisory authorities that provide for handling of individual complaints and dispute resolution; or (3) commitment to cooperate with data protection authorities located in the European Union or their authorized representatives. This list is intended to be illustrative and not limiting. The private sector may design other mechanisms to provide enforcement, so long as they meet the requirements of the Enforcement Principle and the FAQs. Please note that the Enforcement Principle's requirements are additional to the requirement set forth in paragraph 3 of the introduction to the Principles that self- regulatory efforts must be enforceable under Article 5 of the Federal Trade Commission Act or similar statute.

Recourse Mechanisms. Consumers should be encouraged to raise any complaints they may have with the relevant organization before proceeding to independent recourse mechanisms. Whether a recourse mechanism is independent is a factual question that can be demonstrated in a number of ways, for example, by transparent composition and financing or a proven track record. As required by the enforcement principle, the recourse available to individuals must be readily available and affordable. Dispute resolution bodies should look into each complaint received from individuals unless they are obviously unfounded or frivolous. This does not preclude the establishment of eligibility requirements by the organization operating the recourse mechanism, but such requirements should be

[320] http://www.export.gov/safeharbor/eu/eg_main_018382.asp .

transparent and justified (for example to exclude complaints that fall outside the scope of the program or are for consideration in another forum), and should not have the effect of undermining the commitment to look into legitimate complaints. In addition, recourse mechanisms should provide individuals with full and readily available information about how the dispute resolution procedure works when they file a complaint. Such information should include notice about the mechanism's privacy practices, in conformity with the Safe Harbor Principles. They should also co-operate in the development of tools such as standard complaint forms to facilitate the complaint resolution process.

Remedies and Sanctions. The result of any remedies provided by the dispute resolution body should be that the effects of noncompliance are reversed or corrected by the organization, in so far as feasible, and that future processing by the organization will be in conformity with the Principles and, where appropriate, that processing of the personal data of the individual who has brought the complaint will cease. Sanctions need to be rigorous enough to ensure compliance by the organization with the Principles. A range of sanctions of varying degrees of severity will allow dispute resolution bodies to respond appropriately to varying degrees of non-compliance. Sanctions should include both publicity for findings of non-compliance and the requirement to delete data in certain circumstances. (2) Other sanctions could include suspension and removal of a seal, compensation for individuals for losses incurred as a result of non-compliance and injunctive orders. Private sector dispute resolution bodies and self-regulatory bodies must notify failures of safe harbor organizations to comply with their rulings to the governmental body with applicable jurisdiction or to the courts, as appropriate, and to notify the Department of Commerce (or its designee).

FTC Action. The FTC has committed to reviewing on a priority basis referrals received from privacy self-regulatory organizations, such as BBBOnline and TRUSTe, and EU Member States alleging non-compliance with the Safe Harbor Principles to determine whether Section 5 of the FTC Act prohibiting unfair or deceptive acts or practices in commerce has been violated. If the FTC concludes that it has reason[s] to believe Section 5 has been violated, it may resolve the matter by seeking an administrative cease and desist order prohibiting the challenged practices or by filing a complaint in a federal district court, which if successful could result in a federal court order to same effect. The FTC may obtain civil penalties for violations of an administrative cease and desist order and may pursue civil or criminal contempt for violation of a federal court order. The FTC will notify the Department of Commerce of any such actions it takes. The Department of Commerce encourages other government bodies to notify it of the final disposition of any such referrals or other rulings determining adherence to the Safe Harbor Principles.

Persistent Failure to Comply. If an organization persistently fails to comply with the Principles, it is no longer entitled to benefit from the safe harbor. Persistent failure to comply arises where an organization that has self-certified to the Department of Commerce (or its designee) refuses to comply with a final determination by any self- regulatory or government body or where such a body determines that an organization frequently fails to comply with the Principles to the point where its claim to comply is no longer credible. In these cases, the organization must promptly notify the Department of Commerce (or its designee) of such facts. Failure to do so may be actionable under the False Statements Act (18 U.S.C. § 1001).

The Department (or its designee) will indicate on the public list it maintains of organizations self-certifying adherence to the Safe Harbor Principles any notification it receives of persistent failure to comply, whether it is received from the organization itself, from a self-regulatory body, or from a government body, but only after first providing thirty (30) days' notice and an opportunity to respond to the organization that has failed to comply. Accordingly, the public list maintained by the Department of Commerce (or its designee) will make clear which organizations are assured and which organizations are no longer assured of safe harbor benefits.

An organization applying to participate in a self-regulatory body for the purposes of re-qualifying for the safe harbor must provide that body with full information about its prior participation in the safe harbor.

1 Dispute resolution bodies are not required to conform with the enforcement principle. They may also derogate from the Principles where they encounter conflicting obligations or explicit authorizations in the performance of their specific tasks.

2 Dispute resolutions bodies have discretion about the circumstances in which they use these sanctions. The sensitivity of the data concerned is one factor to be taken into consideration in deciding whether deletion of data should be required, as is whether an organization has collected, used or disclosed information in blatant contravention of the Principles.[321]

10.12 FAQ Choice -Timing of Opt Out

Does the Choice Principle permit an individual to exercise choice only at the beginning of a relationship or at any time?

Generally, the purpose of the Choice Principle is to ensure that personal information is used and disclosed in ways that are consistent with the individual's expectations and choices. Accordingly, an individual should be able to exercise "opt out" (or choice) of having personal information used for direct marketing at any time subject to reasonable limits established by the organization, such as giving the organization time to make the opt out effective. An organization may also require sufficient information to confirm the identity of the individual requesting the "opt out." In the United States, individuals may be able to exercise this option through the use of a central "opt out" program such as the Direct Marketing Association's Mail Preference Service. Organizations that participate in the Direct Marketing Association's Mail Preference Service should promote its availability to consumers who do not wish to receive commercial information. In any event, an individual should be given a readily available and affordable mechanism to exercise this option.

Similarly, an organization may use information for certain direct marketing purposes when it is impracticable to provide the individual with an opportunity to opt out before using the information, if the organization promptly gives the individual such opportunity at the same time (and upon request at any time) to decline (at no cost to the individual) to receive any further direct marketing communications and the organization complies with the individual's wishes.[322]

10.13 FAQ Travel Information

When can airline passenger reservation and other travel information, such as frequent flyer or hotel reservation information and special handling needs, such as meals to meet religious requirements or physical assistance, be transferred to organizations located outside the EU?

Such information may be transferred in several different circumstances. Under Article 26 of the Directive, personal data may be transferred "to a third country which does not ensure an adequate level of protection within the meaning of Article 25(2)" on the condition that it (1) is necessary to provide the services requested by the consumer or to fulfill the terms of an agreement, such as a "frequent flyer" agreement; or (2) has been unambiguously consented

[321] http://www.export.gov/safeharbor/eu/eg_main_018383.asp .

[322] http://www.export.gov/safeharbor/eu/eg_main_018384.asp .

to by the consumer. U.S. organizations subscribing to the safe harbor provide adequate protection for personal data and may therefore receive data transfers from the EU without meeting those conditions or other conditions set out in Article 26 of the Directive. Since the safe harbor includes specific rules for sensitive information, such information (which may need to be collected, for example, in connection with customers' needs for physical assistance) may be included in transfers to safe harbor participants. In all cases, however, the organization transferring the information has to respect the law in the EU Member State in which it is operating, which may inter alia impose special conditions for the handling of sensitive data.[323]

10.14 FAQ Pharmaceutical and Medical Products

1. If personal data are collected in the EU and transferred to the United States for pharmaceutical research and/or other purposes, do Member State laws or the Safe Harbor Principles apply?

Member State law applies to the collection of the personal data and to any processing that takes place prior to the transfer to the United States. The Safe Harbor Principles apply to the data once they have been transferred to the United States. Data used for pharmaceutical research and other purposes should be anonymized when appropriate.

2. Personal data developed in specific medical or pharmaceutical research studies often play a valuable role in future scientific research. Where personal data collected for one research study are transferred to a U.S. organization in the safe harbor, may the organization use the data for a new scientific research activity?

Yes, if appropriate notice and choice have been provided in the first instance. Such a notice should provide information about any future specific uses of the data, such as periodic follow-up, related studies, or marketing. It is understood that not all future uses of the data can be specified, since a new research use could arise from new insights on the original data, new medical discoveries and advances, and public health and regulatory developments. Where appropriate, the notice should therefore include an explanation that personal data may be used in future medical and pharmaceutical research activities that are unanticipated. If the use is not consistent with the general research purpose(s) for which the data were originally collected, or to which the individual has consented subsequently, new consent must be obtained.

3. What happens to an individual's data if a participant decides voluntarily or at the request of the sponsor to withdraw from the clinical trial?

Participants may decide or be asked to withdraw from a clinical trial at any time. Any data collected previous to withdrawal may still be processed along with other data collected as part of the clinical trial, however, if this was made clear to the participant in the notice at the time he or she agreed to participate.

4. Pharmaceutical and medical device companies are allowed to provide personal data from clinical trials conducted in the EU to regulators in the United States for regulatory and supervision purposes. Are similar transfers allowed to parties other than regulators, such as company locations and other researchers?

[323] http://www.export.gov/safeharbor/eu/eg_main_018385.asp .

Yes, consistent with the Principles of Notice and Choice.

5. To ensure objectivity in many clinical trials, participants, and often investigators, as well, cannot be given access to information about which treatment each participant may be receiving. Doing so would jeopardize the validity of the research study and results. Will participants in such clinical trials (referred to as "blinded" studies) have access to the data on their treatment during the trial?

No, such access does not have to be provided to a participant if this restriction has been explained when the participant entered the trial and the disclosure of such information would jeopardize the integrity of the research effort. Agreement to participate in the trial under these conditions is a reasonable forgoing of the right of access. Following the conclusion of the trial and analysis of the results, participants should have access to their data if they request it. They should seek it primarily from the physician or other health care provider from whom they received treatment within the clinical trial, or secondarily from the sponsoring company.

6. Does a pharmaceutical or medical device firm have to apply the Safe Harbor Principles with respect to notice, choice, onward transfer, and access in its product safety and efficacy monitoring activities, including the reporting of adverse events and the tracking of patients/subjects using certain medicines or medical devices (e.g. a pacemaker)?

No, to the extent that adherence to the Principles interferes with compliance with regulatory requirements. This is true both with respect to reports by, for example, health care providers, to pharmaceutical and medical device companies, and with respect to reports by pharmaceutical and medical device companies to government agencies like the Food and Drug Administration.

7. Invariably, research data are uniquely key-coded at their origin by the principal investigator so as not to reveal the identity of individual data subjects. Pharmaceutical companies sponsoring such research do not receive the key. The unique key code is held only by the researcher, so that he/she can identify the research subject under special circumstances (e.g. if follow-up medical attention is required). Does a transfer from the EU to the United States of data coded in this way constitute a transfer of personal data that is subject to the Safe Harbor Principles?

No. This would not constitute a transfer of personal data that would be subject to the Principles.[324]

10.15 FAQ Public Record and Publicly Available Information

Is it necessary to apply the Notice, Choice and Onward Transfer Principles to public record information or publicly available information?

It is not necessary to apply the Notice, Choice or Onward Transfer Principles to public record information, as long as it is not combined with non-public record information and as long as any conditions for consultation established by the relevant jurisdiction are respected.

Also, it is generally not necessary to apply the Notice, Choice or Onward Transfer Principles to publicly available information unless the European transferor indicates that such

[324] http://www.export.gov/safeharbor/eu/eg_main_018386.asp .

information is subject to restrictions that require application of those Principles by the organization for the uses it intends. Organizations will have no liability for how such information is used by those obtaining such information from published materials.

Where an organization is found to have intentionally made personal information public in contravention of the Principles so that it or others may benefit from these exceptions, it will cease to qualify for the benefits of the safe harbor.[325]

[325] http://www.export.gov/safeharbor/eu/eg_main_018387.asp .

Chapter 11

Bibliography (Annex D)

11.1 Literature

Anderson, Ross: Security *Engineering: A Guide to Building Dependable Distributed Systems* (2nd edition 2008)

Assey, James M. Jr. /
Eleftheriou, Demetrios: *The EU-U.S. Privacy Safe Harbor: Smooth Sailing or Troubled Waters?* 9 CommLaw Conspectus: J. Comm. L & Pol'y 2001, 145-158

Barnitzke, Benno,
Corrales, Marcelo,
Donoghue, Andrew,
Forgó, Nikolaus,
Lawrence, Andy: *D7.2.1.1 Cloud Legal Guidelines*, Optimised Infrastructure Services (OPTIMIS) project, 30 November 2010 http://www.optimis-project.eu/sites/default/files/D7.2.1.1%20OPTIMIS%20Cloud%20Legal%20Guidelines.pdf

Bloustein, Edward: *Privacy as an Aspect of Human Dignity*, 39 New York University Law Review 971 (1964)

Boyd, Virginia: *Financial Privacy in the United States and the European Union: A Path to Trans-Atlantic Regulatory Harmonization*, International Finance Seminar, 2005

Brown, Ian: Oxford Internet Institute, University of Oxford, *Working Paper No. 1: The challenges to European data protection laws and principles of 20 January 2010 in the context of the European Commission's Comparative Study on different approaches to new privacy challenges in particular in the light of Technological developments*

Bygrave, Lee A.: Privacy *Protection in a Global Context – A Comparative Overview*, Published in Scandinavian Studies in Law, 2004, vol. 47, p. 319–348 http://folk.uio.no/lee/publications/Privacy%20in%20global%20context.pdf

Carlson, Caron: *U.S. Firms Find No Haven in Safe Harbor*, eWeek, 19 March 2001 http://www.eweek.com/c/a/Data-Storage/US-Firms-Find-No-Haven-in-Safe-Harbor/

Capurro, Rafael: *Privacy – An Intercultural Perspective, Ethics and Information Technology* (2005)

Cavoukian, Ann: Information & Privacy Commissioner Ontario, Canada, *Privacy by Design - The 7 Foundational Principles*, originally published: August 2009, revised January 2011

Cavoukian, Ann: *Privacy in the clouds. A white paper on privacy and digital identity: Implications for the internet*

Cavoukian, Ann,
Martin E. Abrams,
Taylor, Scott: *Privacy by Design: Essential for Organizational Accountability and Strong Business Practices*

Centre for Information Policy Leadership as Secretariat to the Galway Project: *Data Protection Accountability: The Essential Elements, A Document for Discussion*, October 2009 http://www.ftc.gov/os/comments/privacyroundtable/544506-00059.pdf

Centre for Information Policy Leadership as Secretariat to the Paris Project: *Demonstrating and Measuring Accountability – A Discussion Document, Accountability Phase II – The Paris Project*, October 2010 http://www.huntonfiles.com/files/webupload/CIPL_Accountability_Phase_II_Paris_Project.PDF

Chakraborty, Rajarshi,
Ramireddy, Srilakshmi,
Raghu,T.S.,
Rao, H. Raghav: *The Information Assurance Practices of Cloud Computing Vendors*, published by the IEEE Computer Society 2010

Chuvakin Anton: *Insider Attacks: The Doom of Information Security Methods to thwart insider attacks: products, techniques and policies*, 2002

Chuvakin, Anton: *Observe PCI DSS: How to Audit Application Activity - When Logs Don't Help*, 2011

Clarke, Roger: *Introduction to Dataveillance and Information Privacy, and Definitions of Terms* (Original of 15 August 1997, latest revs. 16 September 1999, 8 December 2005, 7 August 2006)

Clear, Marie: *Falling into the Gap: The European Union's Data Protection Act and Its Impact on U.S. Law and Commerce*, 18 J. Marshall J. Computer & Info 2000. 981.

Connolly, Chris: The *US Safe Harbor – Fact or Fiction?* Galexia Study, December 2008 http://www.galexia.com/public/about/news/about_news-id143.html

Correia, Miguel,

Rocha, Francisco: *Lucy in the Sky without Diamonds: Stealing Confidential Data in the Cloud*, Universidade de Lisboa, Faculdade de Ciˆencias and Carnegie Mellon University – Portugal/US, Instituto Superior T´ecnico / INESC-ID – Portugal, published in proceedings of the The 1st International Workshop on Dependability of Clouds, Data Centers and Virtual Computing Environments (DCDV, with DSN'11), Hong Kong, June 2011

DeCew, Judith: *Privacy*, The Stanford Encyclopaedia of Philosophy (Fall 2008 Edition), Edward N. Zalta (ed.)

Dinan, Desmond: *Ever Closer Union: An Introduction to European Integration* (4th Edition), Palgrave Macmillan, 2010

Dowling, Donald C. Jr.: *International Data Protection and Privacy Law*, White & Case, August 2009 http://www.whitecase.com/files/Publication/367982f8-6dc9-478e-ab2f-5fdf2d96f84a/Presentation/PublicationAttachment/30c48c85-a6c4-4c37-84bd-6a4851f87a77/article_IntlDataProtectionandPrivacyLaw_v5.pdf

Egan, Erin: *Google, FTC Reach "Buzz" Settlement,* Covington & Burling LLP, March 30, 2011 http://www.insideprivacy.com/united-states/today-the-federal-trade-commission/

EuroCloud

Deutschland_eco e. V.: Guidelines Cloud Computing - German Law, Data Protection & Compliance, http://en.eurocloud.de/2011/03/04/eurocloud-guidelines-cloud-computing-german-law-data-protection-and-compliance/

Federal Trade Commission: *Protecting Consumer Privacy in an Era of Rapid Change – a Proposed Framework for Business and Policymakers*, December 2010 http://www.ftc.gov/os/2010/12/101201privacyreport.pdf.

Fink, Simon: *Datenschutz zwischen Staat und Markt. Die „Safe Harbor"-Lösung als Ergebnis einer strategischen Interaktion zwischen der EU, den USA und der IT-Industrie*, master's thesis at the University of Konstanz, 2002

Fitó, J. Oriol,
Guitart, Jordi: *Introducing Risk Management into Cloud Computing*, a paper based on research work supported by the Ministry of Science and Technology of Spain and the European Union (FEDER funds) and by the Generalitat de Catalunya, Barcelona Supercomputing Center and Technical University of Catalonia, Barcelona, Spain http://gsi.ac.upc.edu/apps/reports/2010/33/cnsm10.pdf

Gordon, Philip L.: *Multinationals Certified to the U.S.-E.U. Safe Harbor Agreement Beware: The Federal Trade Commission Has Bared Its Enforcement Teeth*, Littler Workplace Privacy Counsel, Oktober 13th 2009 http://privacyblog.littler.com/2009/10/articles/data-security/multinationals-certified-to-the-useu-safe-harbor-agreement-beware-the-federal-trade-commission-has-bared-its-enforcement-teeth/

Goury, Régine,
Lambert, Laurence Dumure,
Prinsley, Mark A.,
Yaros, Oliver: *New EU Standard Contractual Clauses for Commissioned Data Processing* in Meyer Brown L.L.P. publication of September 2010

Helbing, Thomas: *How the New EU Rules on Data Export Affect Companies in and Outside the EU*, March 26th 2010 http://www.thomashelbing.com/en/how-new-eu-rules-data-export-affect-companies-and-outside-eu

Hess, Andreas: *American social and political Thought: a concise Introduction*, Edinburgh: Edinburgh University Press, 2000

Hoff, Todd: *Intercloud: How will we scale across multiple clouds?*, 5 April 2010 http://highscalability.com/blog/2010/4/5/intercloud-how-will-we-scale-across-multiple-clouds.html

Kobrin, Stephen J.: *Safe harbours are hard to find: the trans-Atlantic data privacy dispute, territorial jurisdiction and global governance*, Review of International Studies (2004), 30, 111–131 http://www-management.wharton.upenn.edu/kobrin/documents/ris%20article.pdf

Kroes, Neelie: European Commission Vice-President for the Digital Agenda, *Cloud Computing and Data Protection*, speech held at Les Assises du Numérique conference, Université Paris-Dauphine, 25 November 2010

Kuan Hon, W., Millard, Christopher, Walden, Ian: *The Problem of 'Personal Data' in Cloud Computing – What Information is Regulated? The Cloud of Unknowing, part 1*, Queen Mary University of London, School of Law Legal Studies Research Paper No. 75/2011

Locke, John: *Two treatises of government*, Book II, Chapter II. Sect. 4 and 6, first published anonymously in 1689

London Economics: *Study on the economic benefits of privacy-enhancing technologies (PETs)*, Final Report to The European Commission DG Justice, Freedom and Security, July 2010 http://ec.europa.eu/justice/policies/privacy/docs/studies/final_report_pets_16_07_10_en.pdf

Lukas, Aaron: *Safe Harbor or Stormy Waters? Living with the EU Data Protection Directive*, Cato Institute's Center for Trade Policy Studies, 2001 http://www.cato.org/pubs/tpa/tpa-016.pdf

Marnau, Ninja, Schlehahn, Eva: *Cloud Computing und Safe Harbor*, DuD 5/2011, pp. 311-316

Mesaikou, Evangelia: *Examining the Binding Corporate Rules as the most promising solution for the cross border data transfers of multinational companies under the EU Data Protection Directive*, Master Thesis, Tilburg Institute for Law, Technology, and Society (TILT), 2008

Michael, James: New Report on Computer Data Banks, New Scientist, November 9, 1978

National Institute of Standards and

Technology (NIST): *Cloud Computing Synopsis and Recommendations*, May 2011 special publication

NEC Company, Ltd.;

Ann Cavoukian: *Modelling Cloud Computing Architecture Without Compromising Privacy: A Privacy by Design* Approach, May 2010

Organisation for

Economic Co-operation

and Development

(OECD): *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*

Pearson, Siani,

Charlesworth, Andrew: *Accountability as a Way Forward for Privacy Protection on the Cloud*, 6 August 2009

Pfitzmann, Andreas,

Hansen, Marit: *A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management*, Version v0.34, Aug. 10, 2010
http://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.34.pdf

Rannenberg, Kai,

Royer, Denis,

Deuker André (ed.): *The Future of Identity in Information Society – Challenges and Opportunities*, FIDIS (Future of Identity in the Information Society) Summit Book, Springer 2009

Reding, Viviane: Vice-President of the European Commission and EU Justice Commissioner, *Your data, your rights: Safeguarding your privacy in a connected world* – speech held at the Privacy Platform "The Review of the EU Data Protection Framework" Brussels, 16 March 2011

Reding, Viviane: *Companies don't take protection of personal data seriously enough*, an interview on strengthening consumer's data protection rights as consequence of data breach cases of Apple and Sony, published 10 May 2011 – Updated 17 May 2011 at euractiv.com (interviewer: Francesco Guarascio)

Reidenberg, Joel R.: Resolving International Data Privacy Rules in Cyberspace, Stanford Law Review 52 (2000), 1315 – 1376

Reidenberg, Joel R.: Testimony before the Subcommittee on Commerce, Trade and Consumer Protection of the Committee on Energy and Commerce of the United States House of Representatives, Hearing on the EU Data Protection Directive: Implications for the U.S. Privacy Debate, March 8, 2001
http://reidenberg.home.sprynet.com/Reidenberg_Testimony_03-08-01.htm

Reidenberg, Joel R./
Paul M. Schwartz: *Data Protection Law and On-Line Services*: Regulatory Responses, 1998
http://www.paulschwartz.net/pdf/onlinesvcs_schwartz-reidenberg.pdf

Robinson, Neil,
Valeri, Lorenzo,
Cave, Jonathan,
Starkey, Tony,
Graux, Hans: *The Cloud: Understanding the Security, Privacy and Trust Challenges* – Final Report for Directorate-General Information Society and Media, European Commission, 30 November 2010

San Martin,
Cristos Velasco: *Jurisdictional aspects of Cloud Computing*, Director General of the North American Consumer Project on Electronic Commerce (NACPEC), February 28, 2009

Schild, Rebecca: *Does the Safe-Harbor Program Adequately Address Third Parties Online?* Centre for Internet and Society, April 16th 2010
http://www.cis-india.org/advocacy/igov/blog/does-the-safe-harbor-program-adequately-address-third-parties-online

Schoeman, F. (ed.): *Philosophical Dimensions of Privacy: An Anthology*, Cambridge University Press, 1984

Schriver, Robert R.: *You Cheated, You Lied: The Safe Harbor Agreement and its Enforcement by the Federal Trade Commission*; Fordham L. Rev. 2002, Volume 70, Issue 6, 2777
http://ir.lawnet.fordham.edu/flr/vol70/iss6/29

Segalis, Boris: FTC Takes a Big Step in Privacy Enforcement with Google Buzz Settlement, April 6, 2011
http://www.infolawgroup.com/2011/04/articles/enforcement/ftc-takes-a-big-step-in-privacy-enforcement-with-google-buzz-settlement/

Simitis, Spiros: *Establishing International Structures to Monitor and Enforce Data Protection*, in: Policy Issues in Data Protection and Privacy, Paris 1974

Smith, Robert Ellis: *Ben Franklin's Web Site 6*, Sheridan Books 2000

Takatori, Wakako: *Cross-border Trade of Personal Data: Impact of Privacy Laws on the Private Sector and Analysis under GATS Framework*, 2010

Uhl, Antje-Kathrin,
Kern, Reinhold: *Datenmissbrauch am Arbeitsplatz – eine Herausforderung für Personalmanager*, German study of CMS Hasche Sigle in cooperation with Kroll Ontrack, published on 22 March 2011 http://www.cms-hs.com/NewsMedia/PressReleases/Documents/2011_03_Studie_CMS-Kroll_Ontrack.pdf

van Dijk, Marten,
Juels, Ari: *On the Impossibility of Cryptography Alone for Privacy-Preserving Cloud Computing*, published in proceedings of the 5th USENIX Conference on Hot Topics in Security, pages 1–8, 2010

White, Aoife *IP Addresses Are Personal Data, E.U. Regulator Says*, published in The Washington Post on 22 January 2008 http://www.washingtonpost.com/wp-dyn/content/article/2008/01/21/AR2008012101340.html

Whittaker, Zack Dutch *government to ban U.S. providers over Patriot Act concerns*,
published 19 September 2011
http://www.zdnet.com/blog/btl/dutch-government-to-ban-us-providers-over-patriot-act-concerns/58342

Patriot Act affects European cloud adoption,
published 2 August 2011
http://www.zdnet.com/blog/btl/dutch-government-to-ban-us-providers-over-patriot-act-concerns/58342

Wybitul, Tim,
Dr. Patzak, Andrea,
Dr. Zeppenfeld, Guido: *Legal Update*, July 22nd 2010, Mayer Brown http://www.mayerbrown.com/publications/article.asp?id=9377&nid=6

Zhang, Liang-Jie,

Zhou, Qun: *Introduction to Cloud Computing Open Architectures as a new model of SOA's: CCOA: Cloud Computing Open Architecture*, published for 2009 IEEE International Conference on Web Services

11.2 Legislation

Bundesdatenschutzgesetz - German Federal Data Protection Act (BDSG), in the version promulgated on 14 January 2003 (Federal Law Gazette I, p. 66), last amended by Article 1 of the Act of 14 August 2009 (Federal Law Gazette I, p. 2814), in force from 1 September 2009

http://www.bfdi.bund.de/EN/DataProtectionActs/Artikel/BDSG_idFv01092009.pdf?__blob=publicationFile

Charter of Fundamental Rights of the European Union (2000/C 364/01), proclaimed on 7th December 2000 by the European Parliament, the Council of Ministers and the European Commission, with full legal effect since the entry into force of the Lisbon Treaty 1st December 2009, http://www.europarl.europa.eu/charter/pdf/text_en.pdf

Codice in material di protezione dei dati (personali Decreto legislativo 30 giugno 2003, n. 196) – Italian legislative decree for data protection of 30th July 2003

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 (hereinafter referred to as: EU Data Protection Directive 95/46/EC)

Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC (hereinafter referred to as: E-Privacy Directive) concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws

Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (hereinafter referred to as: EU Data retention Directive 2006/24/EC)

European Convention on the Protection of Human Rights and fundamental Freedoms, as amended by Protocol No. 11 (Rome, 4.XI.1950)

Treaty on the functioning of the European Union, in its consolidated and renamed version, entry into force 1st December 2009, as amended by the Treaty of Lisbon and all preceding treaties

11.3 Case law

Census decision of the German Federal Constitutional Court (in German: Volkszählungsurteil Bundesverfassungsgericht) of 15th December 1983 (Az.: 1 BvR 209, 269, 362, 420, 440, 484/83)

Czech Constitutional Court, decision of March 31st 2011 on the national implementation of the Directive in the Czech Republic (Pl. ÚS 24/10 – 94/2011 Coll.)

European Court of Justice (Second Chamber), decision of 4 July 1985 in the case Gunter Berkholz v Finanzamt Hamburg-Mitte-Altstadt, p. 2265 (C-168/84)

European Court of Justice (Fifth Chamber), decision of 7 May 1998 in the case Lease Plan Luxembourg SA v Belgium (C-390/96)

11.4 Official statements & opinions on EU and national level

European Commission

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 (2000/520/EC)*

Commission Decision *of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC (2001/497/EC)*

Commission Decision *of 27 December 2001 on standard contractual clauses for the transfer of personal data to processors established in third countries, under the Directive 95/46/EC (2002/16/EC)*

Commission Decision *of 27 December 2004, amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries (2004/915/EC)*

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 (2010/87/EU)*

Commission Expert Group on European Contract Law, *Feasibility study for a future instrument in European Contract Law*, 3 May 2011

Commission of the European Communities, *First report on the implementation of the Data Protection Directive (95/46/EC)*, Brussels, 15.5.2003

European Commission, Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, A *Digital Agenda for Europe,* Communication COM (2010) 245 of 19 May 2010 *http://ec.europa.eu/information_society/digital-agenda/documents/digital-agenda-communication-en.pdf*

European Commission, Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, *A comprehensive approach on personal data protection in the European Union*, Communication COM (2010) 609 final of 4 November 2010 http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf

European Commission study on *Different approaches to new privacy challenges, in particular in the light of technological developments*, 20 January 2010

European Commission, Directorate-General Justice, *Summary of replies to the public consultation about the future legal framework for protecting personal data*, Brussels, 4 November 2010

Other bodies on European level

Council of Europe, *Explanatory Report to the Convention on Cybercrime* (ETS No. 185)

European Data Protection Supervisor Peter Hustinx, *Opinion on the Communication from the Commission to the European Parliament and the Council - "The EU Counter-Terrorism Policy: main achievements and future challenges"* of 24 November 2010

European Data Protection Supervisor Peter Hustinx, *Opinion on the Evaluation report from the Commission to the Council and the European Parliament on the Data Retention Directive (Directive 2006/24/EC)* of 31 May 2011

European Network and Information Security Agency (ENISA), *Data breach notifications in the EU*, published January 13, 2011

European Network and Information Security Agency (ENISA), *Cloud Computing - Benefits, Risks and Recommendations for Information Security*, published November 20, 2009

European Union Agency for Fundamental Rights, *Access to justice in Europe: an overview of challenges and opportunities*, 23 March 2011

European Union Agency for Fundamental Rights, *Data Protection in the European Union: the role of National Data Protection Authorities - Strengthening the fundamental rights architecture in the EU II*, 2 February 2011

Article 29 Data Protection Working Party

Article 29 Data Protection Working Party, **WP 74**, *Working document: Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers*, adopted on 3rd June 2003

http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2003/wp74_en.pdf

Article 29 Data Protection Working Party, **WP 107**, *Working Document Setting Forth a Co-Operation Procedure for Issuing Common Opinions on Adequate Safeguards Resulting From "Binding Corporate Rules"*, adopted on 14 April 2005

http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp107_en.pdf

Article 29 Data Protection Working Party, **WP 108**, *Working Document Establishing a Model Checklist Application for Approval of Binding Corporate Rules*, adopted on 14 April 2005

http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp108_en.pdf

Article 29 Data Protection Working Party, **WP 133**, *Recommendation 1/2007 on the Standard Application for Approval of Binding Corporate Rules for the Transfer of Personal Data*, adopted on 10 January 2007

http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp133_en.doc

Article 29 Data Protection Working Party, **WP 136**, *Opinion 4/2007 on the concept of personal data*, adopted on 20th June 2007

http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf

Article 29 Data Protection Working Party, **WP 147**, *Working Document 1/2008 on the protection of children's personal data (General guidelines and the special case of schools), adopted on 18 February 2008*

http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp147_en.pdf

Article 29 Data Protection Working Party, **WP 148**, *Opinion 1/2008 on data protection issues related to search engines*, adopted on 4 April 2008

http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp148_en.pdf

Article 29 Data Protection Working Party, **WP 153**, *Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules*, adopted on 24 June 2008

http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp153_en.pdf

Article 29 Data Protection Working Party, **WP 154**, *Working Document Setting up a framework for the Structure of Binding Corporate Rules*, adopted on 24 June 2008

http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp154_en.pdf

Article 29 Data Protection Working Party, **WP 155 rev.04**, *Working Document on Frequently Asked Questions (FAQs) related to Binding Corporate Rules*, adopted on 24 June 2008 as last revised and adopted on 8 April 2009

http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp155_rev.04_en.pdf

Article 29 Data Protection Working Party, **WP 161**, *Opinion 3/2009 on the Draft Commission Decision on standard contractual clauses for the transfer of personal data to processors established in third countries, under Directive 95/46/EC (data controller to data processor)*, adopted on 5 March 2009

http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp161_en.pdf

Article 29 Data Protection Working Party in cooperation with Working Party on Police and Justice, **WP 168**, *The Future of Privacy - Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data*, adopted on 01 December 2009

http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_en.pdf

Article 29 Data Protection Working Party, **WP 169**, *Opinion 1/2010 on the concepts of "controller" and "processor", adopted on 16 February 2010*

http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf

Article 29 Data Protection Working Party, **WP 172**, *Report 01/2010 on the second joint enforcement action: Compliance at national level of Telecom Providers and ISPs with the obligations required from national traffic data retention legislation on the legal basis of Articles 6 and 9 of the e-Privacy Directive 2002/58/EC and the Data Retention Directive 2006/24/EC amending the e-Privacy Directive, adopted on 13 July 2010*

http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp172_en.pdf

Article 29 Data Protection Working Party, **WP 173**, *Opinion 3/2010 on the principle of accountability*, adopted on 13 July 2010

http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_en.pdf

Article 29 Data Protection Working Party, **WP 174**, *Opinion 4/2010 on the European code of conduct of FEDMA for the use of personal data in direct marketing*, adopted on 13 July 2010

http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp174_en.pdf

Article 29 Data Protection Working Party, **WP 176**, *FAQs in order to address some issues raised by the entry into force of the EU Commission Decision 2010/87/EU 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, adopted on 12 July 2010

http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp176_en.pdf

Article 29 Data Protection Working Party, **WP 179**, *Opinion 8/2010 on applicable law*, adopted on 16 December 2010

http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp179_en.pdf

Article 29 Data Protection Working Party, **WP 184**, *Working Document 01/2011 on the current EU personal data breach framework and recommendations for future policy developments*, adopted on 5 April 2011

http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp184_en.pdf

Article 29 Data Protection Working Party, **WP 185**, *Opinion 13/2011 on Geolocation services on smart mobile devices*, adopted 16 May 2011

http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp185_en.pdf

Article 29 Data Protection Working Party, **WP 187**, *Opinion 15/2011 on the definition of consent*, adopted on 13 July 2011

http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf

Article 29 Data Protection Working Party **press release of 2 October 2008** "The Article 29 Data Protection Working Party held its 67th plenary session in Brussels on October 2 - Continuing the efforts for the reinforcement of Binding Corporate Rules",

http://ec.europa.eu/justice/policies/privacy/news/docs/pr_02_10_08_en.pdf

Article 29 Data Protection Working Party **press release of 11 April 2011** about the 80th plenary meeting on 4 and 5 April 2011 in Brussels

http://ec.europa.eu/justice/policies/privacy/news/docs/pr_11_04_11_en.pdf

National Level

Ad-hoc Working Group "Konzerninterner Datenverkehr" (Intra-group data transfer), which was constituted by initiative of the Duesseldorfer Kreis (decisive panel of the German supreme supervisory authorities for data protection in the non-public sector), *Working report of 11 January 2005 inter alia on company-internal data transfers*

Datatilsynet (Danish Data Protection Agency Copenhagen K), *Regarding processing of confidential and sensitive personal data in conncetion with use of Google Apps online office suit* (3 February 2011)

Duesseldorfer Kreis Resolution - *Decision by the supreme supervisory authorities for data protection in the nonpublic sector on 28/29 April 2010 in Hannover [revised version of 23 August 2010] - Examination of the data importer's self-certification according to the Safe-Harbor-Agreement by the company exporting data for data protection in the non-public sector about Safe Harbor*

The National IT and Telecom Agency Copenhagen, Denmark, *New Digital Security Models - Discussion Paper*, February 2011

White House: *A Framework for Global Electronic Commerce*, 1997
http://www-e-jus.it/db/data/Framework_Electronic_commerce_1-7-97.htm

Working group "Internationaler Datenverkehr" ("International data transfer") of the German data protection authorities – *German version of position paper of 28 March 2007 in regard to the European standard contractual clauses*:

https://www.ldi.nrw.de/mainmenu_Service/submenu_Entschliessungsarchiv/Inhalt/Beschluesse_Duesseldorfer_Kreis/Inhalt/2007/20070419_Internationaler_Datenverkehr/Positionspapier.pdf

Chapter 12

List of Abbreviations (Annex E)

Abbreviation	Definition
BCR	Binding Corporate Rules
CoC	Code of Conduct
CoECC	Council of Europe Convention on Cybercrime
CSP	Cloud Service Provider
DCMA	Digital Millennium Copyright Act (US)
EC	European Commission
EEA	European Economic Area
ENISA	European Network and Information Security Agency
EU	European Union
EU SCC	European Union Standard Contractual Clauses
HIPAA	US Health Insurance Portability and Accountability Act
ICT	Information and Communication Technology
ISAE	International Standard on Assurance Engagements
ISO	International Organisation for Standardisation
ISP	Internet Service Provider
IT	Information Technology
ITIL	IT Infrastructure Library
OECD	Organisation for Economic Co-operation and Development
PbD	Privacy by Design
SAS70II	Statement on Auditing Standards (SAS) No. 70 II
SLA	Service Level Agreement
SOX	US Sarbanes Oxley Act
TClouds	Trustworthy Clouds
TEC	Treaty on European Union
TFEU	Treaty on the Functioning of the European Union
ToS	Terms of Service
VM	Virtual machine