FAKULTÄT FÜR !NFORMATIK
Faculty of Informatics

Security and Legal Aspects of Cloud Computing

DIPLOMARBEIT

zur Erlangung des akademischen Grades

Diplom-Ingenieur

im Rahmen des Studiums

Business Informatics

eingereicht von

Andreas Kronabeter
Matrikelnummer 0525182

an der
Fakultät für Informatik der Technischen Universität Wien

Betreuung
Betreuer: Ao.Univ.Prof.Dr. Wolfgang Kastner

Wien, 19.01.2015

(Unterschrift Verfasser/in) (Unterschrift Betreuer)

Erklärung zur Verfassung der Arbeit

Andreas Kronabeter
Schmalzhofgasse 18/34
1060 Wien

Hiermit erkläre ich, dass ich diese Arbeit selbständig verfasst habe, dass ich die verwendeten Quellen und Hilfsmittel vollständig angegeben habe und dass ich die Stellen der Arbeit - einschließlich Tabellen, Karten und Abbildungen -, die anderen Werken oder dem Internet im Wortlaut oder dem Sinn nach entnommen sind, auf jeden Fall unter Angabe der Quelle als Entlehnung kenntlich gemacht habe.

Wien, 19.01.2015 _____

(Unterschrift Verfasser/in)

Expression of thanks

Diese Diplomarbeit möchte ich meiner Mutter Monika Kronabeter und meinem Vater Erich Kronabeter widmen.

Abstract

Cloud computing became an important and ubiquitous term in the world of information technology and telecommunication. Cloud computing must not be necessarily seen as a new invention, rather as a unification of already existing technologies and an evolution out of different concepts like Grid Computing and Utility Computing which will be described in the work. The essential characteristics of cloud computing such as elasticity or broad network access provide many economic benefits for their users, but with these benefits also many security and privacy risks come along. These risks can be generally classified into legal and technical issues. Within this work, a framework for the evaluation of cloud computing providers based on standardized requirements and risks is presented and used for an evaluation of the cloud market. The now adopted general data protection regulation by the European Parliament is a step forward to a secure handling of cloud services and minimization of the related risks. We further describe a framework for cloud service providers in regard to the general data protection regulation. The framework shall help organizations to comply with it according to described security issues.

Kurzfassung

Cloud Computing wurde zu einem wichtigen und allgegenwärtigen Begriff in der Welt der Informationstechnologie. Cloud Computing muss aber nicht unbedingt als eine neue Erfindung angesehen werden. Es ist vielmehr eine Vereinigung von bereits vorhandenen Technologien bzw. eine Evolution von Konzepten, wie zum Beispiel Grid Computing oder Utility Computing, die in dieser Arbeit beschrieben werden. Die wesentlichen Merkmale von Cloud Computing wie Elastizität oder die Möglichkeit des umfassenden Netzwerkzugriffs, bieten Nutzern viele wirtschaftliche Vorteile. Jedoch bringt Cloud Computing nicht nur Vorteile sondern auch Risiken im Bereich der Sicherheit und dem Schutz von Daten mit sich. Generell können diese Risiken in rechtliche und technische Belange unterteilt werden. Mit dieser Arbeit wird ein Rahmenwerk zur Bewertung von Cloud Computing Anbietern auf Basis standardisierter Anforderungen und Risiken dargestellt und für eine Bewertung des derzeitigen Cloud Marktes herangezogen. Die Adaption der Datenschutzverordnung des Europäischen Parlaments ist mit Sicherheit ein wichtiger und richtiger Schritt hinsichtlich eines sicheren Umgangs mit Cloud Services zur Minimierung der damit verbundenen Risiken. Des Weiteren wird in dieser Arbeit für Cloud Service Anbieter ein Rahmenwerk in Bezug auf die allgemeinen Datenschutzregelung definiert und erklärt.

Contents

CHAPTER 1

Introduction and Motivation

1.1 Statement of the Problem

Cloud computing became an important and ubiquitous term in the world of *Information Technology (IT)* and *Telecommunication*. There is no doubt that the hype about cloud computing will continue. Dozens of people and companies are already using services or networks provided over *"the Cloud"* and the number is still growing. However, what is behind all this cloud hype?

At first, it is important to mention that cloud computing must not be necessarily seen as a new invention, rather as a unification of already existing technologies or concepts like *Grid Computing*, *Utility Computing*, or *Distributed Systems* which will be further described in this work.

> "In reality, the cloud is something that you have been using for a long time now; it is the Internet, along with all the associated standards and protocols that provide a set of Web services to you." [Sos11, p. XXV]

The technological progress in the area of information technology is growing very fast, the result is that we have nowadays the technical requirements for the realization of cloud computing.

The basic idea is to offer storage and processing power on-demand over the Internet. That gives companies the possibility to amend their IT-Infrastructure or completely outsource it to the cloud. The offered infrastructure can be, for instance, calculating capacity, data storage, ready-made software. Furthermore, the aim of cloud computing is to use services scalable and dynamic, in other words, to use external hardware and software, and simultaneously economize resources to be more flexible. Hence, cloud computing offers developers innovative ideas to build up their applications and enterprise much easier due to the possibility of using resources from a third party. That said

companies do not have to invest any longer a lot of money in hardware and can focus on their business ideas. The infrastructure in a cloud can grow simultaneously and on-demand with the growth of the users' needs [CB11, p. 1-2]. In simple terms: it is more efficient for organizations to use the offered IT capabilities from a third party as owning and operating their own servers and software [RSA09, p. 1].

We described now the basic idea of cloud computing but it also comes along with some uncertainties regarding the issues: data privacy, data protection as well as security and reliability of the provider and the offered services.

> "As companies migrate their IT infrastructure to the cloud, they effectively relinquish some control over their information infrastructure and processes, even while they are required to bear greater responsibility for data confidentiality and compliance." [RSA09, p. 1]

The quotation above describes the loss of control when using services via cloud computing. A customer does not control anymore his data and processes which are outsourced to a third party. Hence, users are confronted with many regulatory compliance issues based on the problem that different countries have a different legal basis regarding cloud computing and data protection. The topic compliance of cloud computing is still in some way a wild disorder. Companies which are deploying cloud services transnational in different countries or users who are using services have to deal with multiple jurisdictions [Sos11, p. 19].

1.2 Related Work

The different areas of relevance have been already analyzed in the literature. The National Institute of Standards and Technologies (NIST) summarized security and privacy issues and recommendations an organization should follow in their "Guidelines on Security and Privacy in Public Cloud Computing" [WJ11]. The different areas are Governance, Compliance, Trust, Architecture, Identity and Management, Software Isolation, Data Protection, Availability, and Incident Response.

The Cloud Security Alliance (CSA) published their "Security Guidance for Critical Areas of Focus in Cloud Computing" with the focus on governing and operating issues [All11]. The governing part includes Governance and Enterprise Risk Management, Legal Issues, Compliance and Audit, Information Management and Data Security, Interoperability and Portability. The operating part includes Traditional Security, Business Continuity, and Disaster Recovery, Data Center Operation, Incident Response, Application Security, Encryption and Key Management, Identity, Entitlement, and Access Management, Virtualization, Security as a Service.

Another approach provides the Australian Government with their "Cloud Computing Security Considerations" [oD11]. In this work, a checklist of questions according to security issues an organization has to deal with when using cloud computing is provided.

Further relevant work about security risks and recommendations comes from Gartner as well as from the European Network and Information Security Agency (ENISA).

All these approaches numerate what an organization has to consider in regard to security and privacy.

1.3 Goal and Structure

The aim of this work is to give an insight about cloud computing and the offered services with the focus on legal aspects (data privacy, data protection, security). The work highlights the main areas of concern and the related information and security risks. Based on these areas of concern, a framework for the evaluation of public cloud computing providers is presented. The framework can be used by cloud customers to get an overview which providers are reliable according to the different areas of concern and regulatory compliance. The evaluation includes privacy, policies, compliance and security issues and should highlight the features of a secure cloud computing provider. Moreover, within this work a framework related to the new proposed data protection regulation by the European Commission is presented. We provide a checklist for general security and privacy considerations as well as for legal considerations and requirements according to the upcoming general data protection regulation.

The research questions for this work are:

- What is the definition of a secure cloud computing provider?
- What are the legal requirements for offering cloud computing?
- Which risks and concerns arise with the use of cloud computing?
- What are the characteristics of a secure cloud computing provider?
- How can provider comply with the proposed EU data protection regulation?

The work is divided into six chapters. The first chapter includes the *Introduction and Motivation* for this work. The second chapter *Cloud Computing* discusses the fundamentals of cloud computing and different definitions are presented. In the third chapter *Legal Bases of Cloud Computing*, the applicable law of contract and the applicable data protection law for Europe and Austria are discussed, in order to get an insight of the legal situation regarding cloud computing. The third chapter describes national and international legal laws and regulations as well as the EU Data Protection Regulation - COM (2012 11) proposed by the European Commission. The fourth chapter *Market Analysis* gives an overview of the cloud computing market situation. Therefore, the

most common providers are explained in detail. Chapter five *Security and Privacy Risks* discusses related work and defines major risks. Chapter six *Frameworks* includes the areas of concerns and the two frameworks: Evaluation Framework and EU Data Protection Regulation Framework. The key aspect is to get an overview of issues like data privacy, data protection and security of the different vendors. Further, the results of the evaluation are presented.

CHAPTER 2

Cloud Computing

This chapter deals with the introduction and idea of *Cloud Computing* and *Cloud Services*. Relevant basics for this work will be defined, different layers and types of cloud computing will be presented, properties and characteristics of cloud computing will be explained. Moreover, a definition of the term cloud computing will be provided. Furthermore, different technologies important for the development of cloud computing such as *Utility Computing* and *Grid Computing* will be explained in the following paragraphs.

2.1 Definition

Cloud computing is not a term or idea which just suddenly accrued, it is more a concept which evolved out of different technical developments over the last decades. Figure 2.1 by [BF10, p. 4] shows the computing paradigm shift in the last decades and the evolutionary change of how services are provided and consumed (from mainframe computing to cloud computing). Phase 1 shows the use of terminals, so that many users could share powerful mainframes. Phase 2 illustrates the stand-alone personal computer (PC), which was already powerful enough for the user's daily work. Local networks used to connect PCs and servers, in order to increase performance and share resources, are shown in phase 3. Phase 4 shows the connection of local networks over the Internet to build a global network, which enabled remote applications and resources. Phase 5 illustrates the concept of grid computing, which enabled shared computing power and storage – this can be pictured as a distributed system. The last phase represents cloud computing, which provides high-end computing power and services over the Internet. At the first glance, it looks like a step back to mainframe computing, but mainframe computing can just provide finite computing power, due to the usage of a physical machine, while cloud computing can offer almost infinite power and capacity [BF10, p. 3-4].

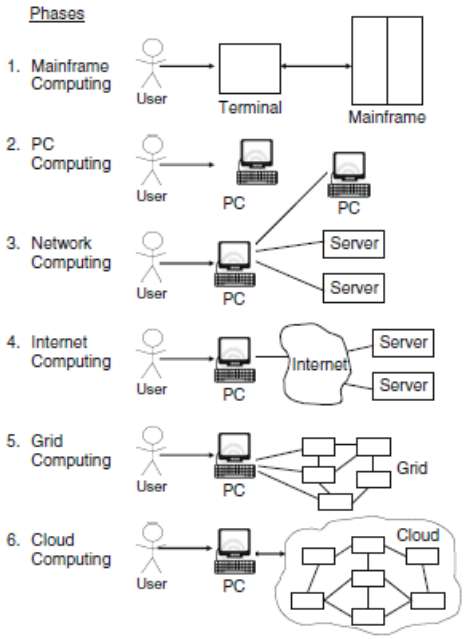

Figure 2.1: Six computing paradigms [BF10, p. 4]

In order to fully understand the evolution and idea of cloud computing it is important to explain the term utility computing.

The idea of utility computing from John McCarthy[1] was to bundle computing resources and to offer it like public utility, such as water and electricity are provided as a public utility.

> "If computers of the kind I have advocated become the computers of the future, then computing may someday be organized as a public utility just as the telephone system is a public utility... The computer utility could become the basis of a new and important industry." *John McCarthy, MIT Centennial in 1961*

Utility computing is rather a kind of business model in which computing resources are offered as metered services, like physical public utilities, than a new concept of computing infrastructure [IF08, p. 2].

The idea and concept of utility computing applies to the computing paradigms cloud computing as well as to grid computing. Before the term cloud computing will be defined the term grid computing has to be explained. In [Fos02], a checklist is presented, where a grid is a system that administrates the computing resources not centrally, uses

[1] John McCarthy(1927 – 2011) was an American computer scientist and pioneer in the field of artificial intelligence.

open standards, and delivers nontrivial quality of service. As a consequence, grid computing occurs in a cloud in dependence of the cloud's type, e.g. the service type Platform as a Service (PaaS) (Chapter 2.3.1) can be delivered by a private cloud. Additionally, the resources from a grid are usually on premise and owned by an organization, which differs from a cloud, because clouds are normally provided by vendors.

> "The evolution has been a result of a shift in focus from an infrastructure that delivers storage and compute resources (such is the case in Grids) to one that is economy based aiming to deliver more abstract resources and services (such is the case in Clouds)." [IF08, p. 2]

The mentioned points show us that the idea of utility computing can be found in the definition of grid computing. This leads us to the definition and difference of cloud computing. Cloud computing is the realization of computing as a utility over the Internet. As already mentioned, cloud computing is not a unified term, many definitions can be found in literature but most of them lead in the same direction and have a similar meaning. In the following paragraphs some of them are presented and discussed.

In [IF08], cloud computing is defined as:

> "A large-scale distributed computing paradigm that is driven by economies of scale, in which a pool of abstracted, virtualized, dynamically-scalable, managed computing power, storage, platforms, and services are delivered on demand to external customers over the Internet." [IF08, p. 1]

The definition by [CB11, p. 4] is similar to the definition above and means that cloud computing uses the virtualization of computing and storage resources and the modern web-technologies, in order to provide platforms and applications as on-demand services, which are scalable and network-centered.

The definition presented in [Sos11, p. 3-4] highlights the properties *Abstraction* and *Virtualization*. Cloud computing is defined as a self-service utility that uses technology, services and applications similar to those on the Internet. Furthermore, the term cloud is divided into two concepts:

The abstraction:

> "Applications run on physical system that are not specified, data is stored in locations that are unknown, administration of systems is outsourced to others, and access by users is ubiquitous." [Sos11, p. 3]

And the virtualization by pooling and sharing resources:

> "System and storage can be provisioned as needed from a centralized infrastructure, costs are assessed on a metered basis, multi-tenancy is enabled, and resources are scalable with agility." [Sos11, p. 3]

The next definition provided by the *National Institute of Standards and Technology*[2] *(NIST)* is commonly accepted and also very detailed:

> "Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models." [LB11, p. 2-1]

In summary, it can be stated that the essential properties of cloud computing which occur in all of the mentioned definitions are:

- virtualization
- abstraction
- flexibility
- scalability
- on-demand network access

Figure 2.2 illustrates the essential points mentioned in the definition of NIST. It shows the separation into the fields *Essential Characteristics*, *Service Models* and the *Deployment Models*. Because of the general acceptance of the NIST definition in the literature, all the three scopes of the visual model will be explained and discussed in the following chapters.

[2]National Institute of Standards and Technology, http://www.nist.gov/index.html, last access: 03.08.2014.

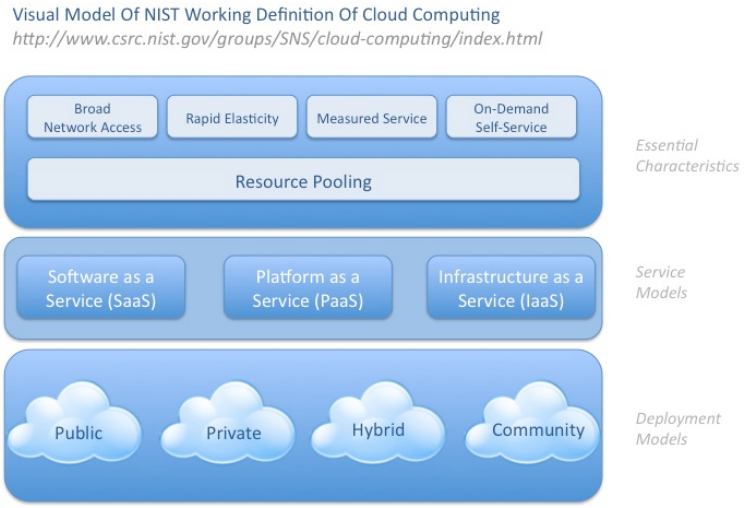

Figure 2.2: Visual Model Of NIST Working Defintion Of Cloud Computing

2.2 Properties and Characteristics

In this Section, the properties and characteristics of cloud computing will be explained. The first scope of the visual model by NIST, as illustrated in Figure 2.2, contains five *Essential Characteristics* [LB11, p. 2-1], namely:

- *Broad network access:* Resources or services are available over the network using standard mechanisms to provide platform independent access (e.g. with mobile phones, laptops, and personal digital assistants (PDAs)).

- *Rapid elasticity:* Resources can be provided rapidly and elastically. It can happen also automatically, depending on the utilization to quickly scale in or to quickly scale out a system. Thus for the customer, it seems that the available capabilities are unlimited and can be purchased in any quantity and at any time.

- *Measured Service:* The use of resources is measured, controlled and optimized by the cloud system automatically, appropriate to the type of service (e.g. bandwidth, storage, processing, active users). Thus, transparency for the provider and consumer is provided.

- *On-demand self-service:* The customer has to register at a service provider and can immediately use the provided computer resources and services. The customer can choose a variety of resources and services and does not need to interact directly with the cloud service provider.

- *Resource pooling:* Resources of the provider are pooled together to offer multi-tenant usage, that means that multiple consumers are served. This is realized with different physical and virtual resources which are allotted according to the customers' needs. Normally the user does not know the location of the provided physical resources like memory, network bandwidth, virtual machines, processing and storage.

Furthermore the five characteristics can be summarized into two concepts which are described in [Sos11, p. 4] as follows:

1. *Abstraction:* Applications run on unspecified physical systems, the location where the data is stored is unknown, the administration is outsourced and the access by users is omnipresent.

2. *Virtualization:* With resource pooling and sharing, cloud computing virtualizes systems. Systems and storage can be provided on-demand, costs are measured by a metered value and resources are scalable with agility.

In comparison to the definition by NIST, the characteristics, on-demand, self-service, and broad network access can be assigned to the concept of Abstraction. Moreover, the characteristics resource pooling, rapid elasticity, and measured services can be classified as Virtualization.

2.3 Cloud Architecture

So far, we discussed the first scope (essential characteristics) of the visual model by NIST (Figure 2.2). In this section, the architecture of cloud computing will be explained.

A cloud architecture consists of *Deployment Models* and *Service Models*. Deployment models reflect the organizational view and service models reflect the technical view of a cloud. Deployment models as organizational view refer to the cloud's infrastructure, its location and on how a cloud is deployed. The service model contains the functional properties and types e.g. how a cloud computing platform is accessible [Sos11, p. 7-10]. In the following two sub chapters, deployment models and service models will be further specified.

2.3.1 Service Models

The second scope of the visual model by NIST are the service models. With the different types of how to access to a cloud computing platform, they build the technical view of cloud computing. There exists three general accepted service types also known as the *SPI MODEL*. SPI stands for: *Software as a Service (SaaS)*, *Platform as a Service (PaaS)*, and *Infrastructure as a Service (IaaS)* [All11, p. 8].

Figure 2.3 illustrates the stack and layered architecture of the three cloud computing service models. In literature, many different definitions of service models exist, but all of them follow the everything-as-a-service-paradigm (XaaS).

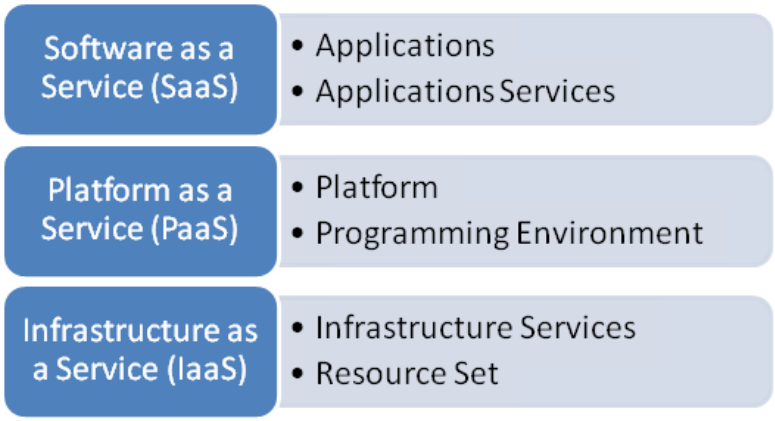

Figure 2.3: Cloud Computing Service Models adapted from [CB11, p. 28]

If we move upwards in the stack of Figure 2.3 each service model inherits the capabilities of the service model beneath it. For a better understanding, IaaS has the lowest level of integrated functionality and integration, on the other hand SaaS has the highest level [Sos11, p. 10].

2.3.1.1 Software as a Service (SaaS)

In the SaaS layer a complete environment is provided. That includes applications, user interface and management, which the client can run remotely from the cloud [Sos11, p. 10] [BF10, p. 5]. The client does not have to install the software locally or to take care about the deployment of the required resources. Hence it is his responsibility to include managing data and user interaction. Everything else from the application to the infrastructure is the responsibility of the provider [Sos11, p. 10]. SaaS consists of the sub layers Applications, and Application Services. The functionality of the application services is just based on one simple application. On the other side, applications are fully-fledged complex applications [CB11, p. 35]. The application is normally provided to the client via an interface, which is usually a browser [Sos11, p. 10]. Examples of SaaS service providers are GoogleApps[3], Oracle On Demad[4] and SalesForce.com[5].

[3]GoogleApps, http://www.google.at/intx/de/enterprise/apps/business/, last access: 03.08.2014.

[4]Oracle CRM On Demand, http://www.oracle.com/us/products/applications/crmondemand/index.html, last access: 03.08.2014.

[5]SalesForce.com, http://www.salesforce.com/, last access: 03.08.2014.

2.3.1.2 Platform as a Service (PaaS)

The cloud services offered in the platform as a service layer are similar to those offered in the infrastructure as a service layer, with the difference that also operating systems and services for the development are included [BF10, p. 5]. The service model provide virtual machines, operating systems, services, applications, transactions, development frameworks, and control structures [Sos11, p. 10]. The services are mostly directed towards developers. PaaS offers environments for developers where client-created software, in specific programming languages are supported by the provider, can be developed and executed [CB11, p. 33].

Furthermore the client does not control the cloud infrastructure but has control over the engaged applications [LB11, p. 2-1].

Examples of PaaS service provider are Microsoft Azure[6], Google App Engine[7], Salesforce's Force.com[8] and GoGrid[9]. In Chapter 4, some of the above mentioned service providers will be further discussed, as part of a market overview.

2.3.1.3 Infrastructure as a Service (IaaS)

The service model IaaS provides computing resources like virtual machines, virtual storage, virtual infrastructure, and other hardware properties as a service for the client [Sos11, p. 10]. Therefore, IaaS consists of the resource set layer, and the infrastructure services layer. In the resources set layer, a user interface is provided to manage a variety of resources and to allocate them for the own usage. Typical features for the user interface are the set up of operation systems (OS) images, the start and stop of OS instances, etc. [CB11, p. 29-30].

For the provision and management of the infrastructure, the service provider is responsible. The client is responsible for other aspects such as the operating system, applications, and the user interactions with the system [Sos11, p. 10]. In doing so, the client does not manage the cloud infrastructure but is controlling the operating system [LB11, p. 2-2].

One layer above the resource set is the infrastructure services layer with a more specific focus on usage. This can be for example infrastructure services for calculation tasks, or mass memory.

As a consequence, the features of IaaS are that the client just has to pay for the needed capacity and can get more if required.

[6] Microsoft Azure, https://azure.microsoft.com, last access: 03.08.2014.
[7] Google App Engine, https://cloud.google.com/appengine/, last access: 03.08.2014.
[8] Force.com, http://www.salesforce.com/platform/what/?d=70130000000lts8, last access: 03.08.2014.
[9] GoGrid, http://www.gogrid.com, last access: 03.08.2014.

Examples of IaaS service providers are Amazon Web Services[10], GoGrid, FlexiScale[11], RackSpace cloud[12] and Microsoft Azure.

2.3.2 Deployment Models

Deployment models are the third scope in the visual model by NIST. A deployment model is an organizational view of cloud computing and its infrastructure. As organizational view of the cloud computing architecture, a deployment model shows how a cloud infrastructure is located as well as the boundary between the clients' and the providers' responsibilities.

According to [LB11, p. 2-2], four types of cloud computing exists: *Public Cloud, Private Cloud, Hybrid Cloud*, and *Community Cloud*.

- *Public Cloud:* The infrastructure of a public cloud (or external cloud) is owned and operated by an organization which is selling cloud services. The public cloud is provided for a large industry group or to the general public. Hence, the vendor and the customer of a public cloud are usually not the same entity.
- *Private cloud:* The infrastructure of a private cloud (or internal cloud) is operated only for one client or one organization. It may be managed by them or a third party and can be either on premise or off premise. Security issues can be one reason for organizations to use a private cloud, because in a private cloud an organization would have full control over their data.
- *Community Cloud:* The infrastructure in a community cloud is shared by various organizations. It supports a specific community with common concerns (e.g. security, mission, policy, requirements and compliance considerations).
- *Hybrid Cloud:* A hybrid cloud is a combination of two or more cloud infrastructures (private, public or community). The particular models remain as a unique entity but are linked together as a unit, by standardized or proprietary technology. This is useful considering security issues, because a hybrid cloud enables to store critical and important information in the public cloud and in case the private clouds is temporarily overloaded the public cloud can be used to provide more processing power.

2.4 Cloud Cube Model

Due to the widespread acceptance and the fact that the definition of cloud computing by NIST is very widely known, we discussed this approach in detail. Another and

[10] Amazon web services, http://aws.amazon.com/, last access: 03.08.2014.
[11] FlexiScale, http://www.flexiscale.com/, last access: 03.08.2014.
[12] RackSpace cloud, http://www.rackspace.com/cloud/, last access: 03.08.2014.

complete different approach of a cloud architecture is the *Cloud Cube Model* from the Jericho Forum[13], as illustrated in Figure 2.4. The Jericho Forum is an association which belongs to the Open Group, with the focus on how to protect cloud networks.

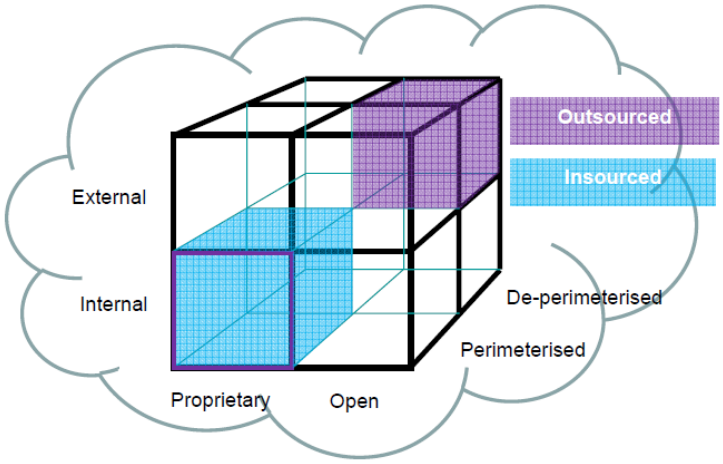

Figure 2.4: The Cloud Cube Model from [For09]

Due to the fact that there are different forms of cloud computing the Jericho Forum tries to provide a model to determine the cloud form which fits most to business needs in respect to the security of data in an abstract way. It categorizes the types of cloud computing and the interaction between the deployment models, service models and physical locations of data and ownership. Their approach of a cloud network is based on four dimensional factors, as illustrated in Figure 2.4 and described below [For09].

- *Internal (I) / External (E):* In this dimension, the physical location of the data is defined, whereby the organizations boundaries will be determined.
- *Proprietary (P) / Open (O):* In this dimension, the state of ownership of interfaces, services, technology, etc. is defined. It serves a gauge for interoperability and technology ownership and enables data transfer between other cloud forms.
- *Permeterised (Per) / De-perimeterised (D-p):* This dimension indicates if the operations are inside of the traditional IT perimeter, like the network firewalls and security boundaries, or outside.
- *Insourced / Outsourced Sourcing:* This dimension has two states. It allows to categorize whether the service is provided from a third party or from the customer.

[13]The Open Group, http://www.opengroup.org/jericho/, last access: 03.08.2014.

2.5 Conclusion

The definition of cloud computing by NIST with the definition of deployment models and service models focus on the delivery of the service from a business perspective. So does the cloud cube model by the Jericho Forum with the difference that they combine the service and deployment model and define it as cloud formation within the four dimensions described before. The main difference between these two models is the level of abstraction. The four dimensions of the cloud cube model enable to define cloud computing formations with a more clearly view on where services will be operated as the NIST model does. On the other side, the NIST model with the definition of hybrid cloud and community cloud provides a definition where deployment models can be combined, which leads to more options than just inside or outside of an organization. If we take the hybrid cloud as a deployment model from the NIST model which is a combination of two or more cloud deployment models it is not possible to illustrate it in the cloud cube model because of the fact that within the four dimension a cloud formation can be either external or internal. The NIST model provides a comprehensive and very detailed definition of cloud computing which can be used to explain the different concepts and characteristics of cloud computing. The cloud cube model by the Jericho Forum does not provide a definition of the characteristics of cloud computing it focuses on the implications of clouds and tries to make the provisioning of cloud services inside and outside of an organization more clear.

Within this chapter, the term and basic concepts of cloud computing necessary for this work are explained. In the next chapter, the subject matter will be cloud computing in the context of law and legal issues.

CHAPTER 3

Legal Bases of Cloud Computing

In the previous chapter, the basis of cloud computing is set from a technical point of view. The focus of this chapter is the relation between cloud computing and law. The legal bases relevant for cloud computing will be explained.

Legal aspects have top priority when discussing cloud computing. Due to cloud computing, many transnational business relationships arise, so that vendor and user are often settled in different countries. This rises a lot of legal questions about contracts, security, data privacy, and compliance. At a glance, the legal bases of cloud computing do not seem to be very transparent.

In this chapter, public clouds are of interest, because they are operated from a third party and the users' data can be stored in a different country (different laws). In contrast, private clouds are normally operated for only one client and operated internally, so no relationship to third parties exists. Hence, their legal bases are not as complicated as with public clouds. A private cloud operated by a service provider can be seen technically as IT-outsourcing [Nie09, p. 446].

The chapter is divided into three parts. The first part is dealing with the law of contract, applicable law, drafting and types of contracts. The second part deals with the data privacy and protection within the European Union and the international legal compliance. In the third part of this chapter, the proposal of 2012 for a reform of the EU's 1995 data protection rules by the European Commission is discussed.

The issues of legal rules and compliance discussed in this chapter rather have their focus on public clouds and companies than on private users.

3.1 Law of Contract

This subchapter will give insights to the applicable law of contract and contracts classifications.

Contracts define the service which has to be performed and the different demands of the contracting parties. Contracts should contain all important agreements, which are necessary to fulfill cloud computing in an approved legal range, such as data privacy and security issues, as well as compliance [Bit10, p. 31]. This means that the conditions between two contract partners have to be clearly defined.

With the standardization of cloud services, there is no provision of an adaption on the individual users' needs [Bit09, p. 48]. This means, that seller and user try to get the best result out of a contract [KT11, p. 185]. Consequently, the user has to agree or disagree with the contract conditions selected by the provider of the cloud service.

3.1.1 Applicable Law

The *Regulation (EC) No 593/2008 (Rome I)*[1] regulates the law applicable to contractual obligations. In situations where a conflict of laws exists, caused by the circumstance that a seller and a user belong to different states, the Rome I regulation should be applied. The regulation shall be applied on contractual obligations in civil and commercial matters, but not on customers' revenues or administrative matters.

The enactment regulates the choice of a national law for transnational contractual relationships under private law. It unifies the existing international private law for all states of the European Union except Denmark.

Referred to in Article 2 (Universal application) Rome I, any law whether or not a law of a member state of the European Union (EU) can be applied by the Rome I regulation. As a consequence, the regulation applies if just one contractual partner has his habitual residence in the EU. The Regulation cannot be applied for domestic situations for example if two companies from the same country ratify a contract without any transnational issues. Furthermore, the Rome I Regulation is not applicable when none of the parties from a given contractual relationship are from the EU.

Referred to in Article 3 (Freedom of choice) of this regulation, contracting parties can choose the applicable law for a contract, but it has to be clearly demonstrated with the terms of the contract. With regard to cloud computing, this is the most common scenario. The choice of law is frequently settled in the general terms and conditions of a contract.

If no law is chosen in accordance with Article 3, then Article 4 (Applicable law in the absence of choice) will be applied. Therefore, Article 4 (1) (b) states

> "a contract for the provision of services shall be governed by the law of the country where the seller has his habitual residence".

[1] Regulation of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:177:0006:0016:En:PDF, last access: 03.08.2014.

In the case that the contract is not a service contract (i.e., the contract is not covered by Article 4 Paragraph 1) then Paragraph 2 will come into effect which states

> "the contract shall be governed by the law of the country where the party required to effect the characteristic performance of the contract has his habitual residence".

In the context of cloud computing, this would be the country of the service provider. Under the circumstance that the contract is more closely connected to a country different from the one indicated in the paragraphs 1 or 2, paragraph 3 states

> "the law of the latter country shall apply".

Finally, Article 4 (4) implies

> "where the law applicable cannot be determined pursuant to paragraphs 1 or 2, the contract shall be governed by the law of the country with which it is most closely connected".

3.1.2 Contract Classification

This subchapter describes the classification of contracts in cloud computing based on the *Austrian civil law (Allgemeines Bürgerliches Gesetzbuch, ABGB)*[2] and the *German civil code (Bürgerliches Gesetzbuch, BGB)*[3].

Contracts of cloud computing rely on the Austrian or German law as long as the habitual residence of the cloud service provider is Austria or Germany. Anyway, this classification will highlight the basic users' rights when ratifying a contract with a provider. International laws and regulations will be discussed later on in the following chapter.

In both laws (ABGB, BGB), different types of obligatory agreements including *lease agreement*, *contract of service agreement*, and *work agreement* [TF10, p. 3] exist.

Regarding cloud computing, all these agreements are important for contracts between a service provider and a user. Usually cloud service contracts are classified as so-called "mixed" agreements, because of the different services or several performance factors which are combined into one uniform contract. Many of the offered services and performances from a provider (e.g. hosting) can be assigned to lease agreements. As mentioned before, in offering a cloud service more goods and facilities are offered, which are either covered by the contract of work (e.g. system maintenance, backups)

[2] Allgemeines bürgerliches Gesetzbuch für die gesammten deutschen Erbländer der Oesterreichischen Monarchie StF: JGS Nr. 946/1811, http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10001622, last access: 03.08.2014.

[3] Bürgerliches Gesetzbuch in der Fassung der Bekanntmachung vom 2. Januar 2002 (BGBl. I S. 42, 2909; 2003 I S. 738), das zuletzt durch Artikel 1 des Gesetzes vom 27. Juli 2011 (BGBl. I S. 1600) geändert worden ist, http://www.gesetze-im-internet.de/bgb/BJNR001950896.html , last access: 03.08.2014.

or the contract of service (e.g. updates, provision of bandwidth) [MS11, p. 71]. Furthermore, it is clear that the description of performance is a very important part for the contract of cloud computing. The different kinds of chosen performances will determine the legal type of a contract [Bit10, p. 31]. The classification is also essential for the design of a contract. Normally it is a standardized contract where the general terms of conditions (GTB) of §305 et seq. BGB and §§864 ABGB et seq. are applicable. Hence the classification decides what is allowed in the GTBs and what is not allowed [MS11, p. 71].

- *Lease agreements:* Most of the performances, like hosting or handing over of software of a cloud service providers are covered under lease agreements [MS11, p. 71]. In law, the time limited access to provided software (cf. SaaS Section 2.3.1.1) represents a kind of *Application Service Providing (ASP)*. According to the *Federal Court of Justice (of Germany)*[4], jurisprudence of the 15.11.2006[5], ASP must be handled as a lease agreement. Additionally, the time limited access to a hosted runtime and development environment (cf. PaaS Section 2.3.1.2) as well as the provision of hardware or storage space (cf. IaaS Section 2.3.1.3) are usually allocated to the meaning of lease agreements [Bit10, p. 40].

  The lease agreement is legally specified in the Austrian civil law under the terms of §§1090 et seq., as well as in the German civil code under the terms of §535 et seq.

- *Contract of service:* Services offered from a provider such as monitoring, operating performance or just support are normally covered by the contract of service [Bit10, p. 40].

  The contract of service is legally specified in the Austrian civil law under the terms of §§1151 et seq., as well as in the German civil code under the terms of §631 et seq.

- *Contract of work:* According to the German Federal Court of Justice judgment of 04. March 2010 - III ZR 79/09, some parts of web-hosting are subject to the meaning of a contract of work. Emphasis is put on the permanent availability of a website [Bit10, p. 40].

  The contract of work is legally specified in the Austrian civil law under the terms of §§1165 et seq., as well as in the German civil code under the terms of §631 et seq.

In summary, it is not always clear which agreement is applicable for an offered service. In the majority of cases, the lease agreement is used, but the allocation of the

[4]Bundesgerichtshof, www.bundesgerichtshof.de, last access: 03.08.2014.

[5]Bundesgerichtshof Urteil vom 15.11.2006 XII ZR 120/04 Rechtsnatur der Softwareüberlassung im Rahmen eines ASP-Vertrages, http://www.jurpc.de/rechtspr/20070001.htm, last access: 03.08.2014.

right law for individual cases depends on how the service is defined and if it includes also other services [Bit10, p. 40].

3.1.3 Service Level Agreements

A *Service Level Agreement (SLA)* is describing the quality of contractual measurable performances, which a provider owes a user. A SLA may occur as an entire contract or as part of a contract. As a part of a contract, SLAs are essential for a contract between two parties. The measured parameter normally is the time, for example, the response time of a system. Moreover, for the non-compliance of an agreement, penalties are defined [MS11, p. 71-72].

In literature, there is no unified perspective about the nature of Service Level Agreements and the way SLAs should be defined, but some similarities about the agreements can be found.

A SLA should at least contain the scope of the agreement (clear defined responsibilities, activities and conditions), services which are clearly defined and sufficient measurable, payment agreements, definition of penalties, security requirements for both parties and the fulfillment of legislative requirements (e.g. data protection law) of the service provider.

3.2 Data Protection

In the first part of this chapter, we discussed the legal bases of cloud computing in the context of the law of contract. This section is about laws and regulations according to cloud computing and will give an overview of different legal regulations according to data protection. It will highlight the requirements for *Controllers* and *Processors*, when dealing with *Personal Data*. Furthermore, laws according to Austria, Europe as well as the US will be explained.

According to Austrian law and German law, data protection refers to the protection of *Personally Identifiable Information* (personal data) against abuse.

For the legal regulations applicable for the protection of processed data, it is important to know where the data is processed. Hence, it is important to distinguish if data are operated and stored in the country where it was generated, or if data are generated and used in different countries. In the first case, the law of that country is applicable (private cloud). In the second case, international and also some national law standards shall be taken into account (public cloud) [Bit10, p. 59-60].

For this section, the following data protection law requirements (if not explicitly mentioned) are generally based on the Austrian Data Protection Law *"Federal Act concerning the Protection of Personal Data - Datenschutzgesetz 2000"* (DSG 2000)[6]. To

[6]Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz 2000 - DSG 2000) BGBl. I Nr. 165/1999 idF BGBl. I Nr. 133/2009 und BGBl. I Nr. 135/2009.

avoid any confusion, in the following chapter, the German title "Datenschutzgesetz 2000" (DSG 2000) will be used. It does exist an English translation but according to the Austrian Data Protection Commission[7], linguistic compromises were unavoidable and only the German version is valid in any legal dispute.

Important terms for the following subsections as defined in the DSG 2000 are:

- *Personal data:* Personal data (§4 (1)) is information about a data subject (§4 (3)) whose identity is determined or determinable. Indirectly personal data are data with the reference to a person so that the identity of the data subject cannot be determined by legal means from a controller (§4 (4)), a processor (§4 (5)) or a recipient of a transmission (§4 (12)).
- *Data subject:* Within the meaning of the DSG 2000, a data subject is any natural or legal person or a group of natural persons, not identical with the controller, whose data is used (§4 (8)).
- *Controller:* A controller is a natural or legal person or a group of natural persons which have taken the decision to use data regardless whether they use the data themselves or to engage a processor to use the data.
- *Processor:* A processor is a natural or legal person, group of persons or organ of a federal, state and local authority which uses data (§4 (8)) for a commissioned work.
- *Use of data:* Use of data is any type of data handling including the processing of data (§4 (9)) as well as the transmission of data (§4 (12)).

3.2.1 Applicable Data Protection Law

In the *European Union* (EU), the *Directive 95/46/EC*[8] is the reference text and basis for the protection law and regulations of personal data. The aim of this directive is to assure the free movement of personal data within the European Union, as unimpeded as possible [Gra10, p. 13].

> "This Directive applies to data processed by automated means (e.g. a computer database of customers) and data contained in or intended to be part of non automated filing systems (traditional paper files)." [9]

[7] Österreichische Datenschutzbehörde, https://www.dsb.gv.at, last access: 03.08.2014.

[8] European Parliament and Council Directive 95/46/EC 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 [Official Journal L 281 of 23.11.1995].

[9] Europa Summaries of EU legislation, http://europa.eu/legislation_summaries/information_society/data_protection/l14012_en.htm, last access: 03.08.2014.

The directive determines the national law applicable in Article 4, which includes the territoriality principle. Referred to in Article 4, the law from the country where the personal data are collected and processed is applicable.

As mentioned, the legal basis for data protection in Austria is regulated by the DSG 2000. Referred to in §3 DSG 2000, the territorial jurisdiction of data protection in Austria is defined according to Article 4 of the European directive. Hence, the Austrian law is principally applicable on every use of data in Austria [Pol10, p. 17], corresponding to the territoriality principle. The technical transit (short term storage) of personal data through a country is permitted according to §3 Art. 3 DSG 2000 [Pol10, p. 18].

Because of the "country of domicile principle" two exceptions exist:

1. If personal data are used in Austria by a controller with a registered headquarter in another State of the *European Economic Area* (EEA)[10] [Gra10, p. 32], then the national law of the controller's country of domicile is applicable. That also includes that the controller has no purpose of using this data for an own establishment (§4 (15)) in Austria. Figure 3.1 illustrates the described exception.

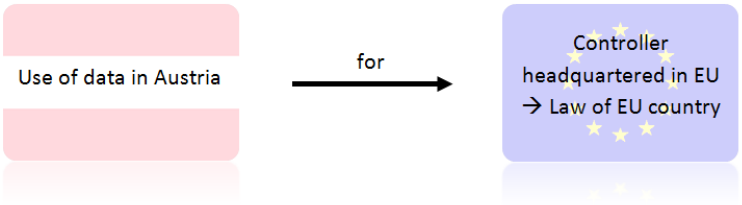

Figure 3.1: Applicable law 2

2. Vice versa, the Austrian law is applicable in another state of the EEA if a controller, having Austria as country of domicile, is using data in another country of the European Union even without having an establishment in that country. The exception is illustrated in Figure 3.2.

The "country of domicile principle" is just applicable on a controller headquartered in a member state of the EU. Outside of the EU, the applicable law is the national law of the country where the data will be processed (Article 4 (1) (c) Directive 95/46/EC) [Pol10, p. 18].

[10]The EEA includes all countries from the European Union plus Norway, Liechtenstein and Island.

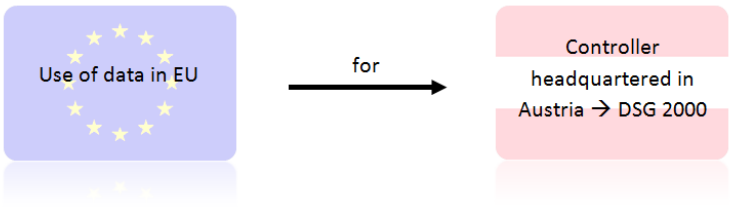

Figure 3.2: Applicable law 2

3.2.2 Data Protection Law – DSG 2000

According to §1 Abs 1 DSG 2000:

> "Everybody shall have the right to secrecy for the personal data concerning him, especially with regard to his private and family life, insofar as he has an interest deserving such protection. Such an interest is precluded when data cannot be subject to the right to secrecy due to their general availability or because they cannot be traced back to the data subject [Betroffener]."[11]

Data which are already generally available (e.g. data from public registers or books as long as they are published permissibly) are excluded [Pol10, p. 13].

Figure 3.3 shows the transmission and committing of personal data according to the DSG 2000 within the context of cloud computing.

3.2.2.1 Committing of data for service processing

According to §10 DSG 2000, controllers are allowed to employ a service provider (processor) for their data applications (§4 (7)), if the service provider guarantees a legitimate and secure use of the data. Therefore, the controller has to make sure that the service provider made every effort to keep all the necessary agreements. Furthermore, the service providers (processors) have according to §11 six obligations using data for a controller:

1. "to use data only according to the instructions of the controller; in particular, the transmission [Übermittlung] of the data used is prohibited unless so instructed by the controller;
2. to take all required safety measures pursuant to §14; in particular to employ only operatives who have committed themselves to confidentiality vis-á-vis the processor or are under a statutory obligation of confidentiality;

[11] Datenschutzgesetz 2000 (DSG 2000), BGBI. I Nr. 165/1999 idF. BGBI. I Nr. 135/2009 (in offizieller englischer Übersetzung), http://www.bka.gv.at/DocView.axd?CobId=41936, last access: 03.08.2014.

3. to enlist another processor only with the permission of the controller and therefore to inform the controller of this intended enlistment of another processor in such a timely fashion that the controller has the possibility to object;
4. insofar as this is possible given the nature of the service processing [Dienstleistung] to create in agreement with the controller the necessary technical and organisational requirements for the fulfilment of the controller's obligation to grant the right of information, rectification and erasure;
5. to hand over to the controller after the end of the service processing all results of processing and documentation containing data or to keep or destroy them on his request;
6. to make available to the controller all information necessary to control the compliance with the obligations according to sub-paras. 1 to 5."

In the case of outsourcing, the controller must check if the international transmission of data is included, to fulfill the approval requirements according to §13. Otherwise he risks to get a sentence according to §52 [Pol10, p. 53].

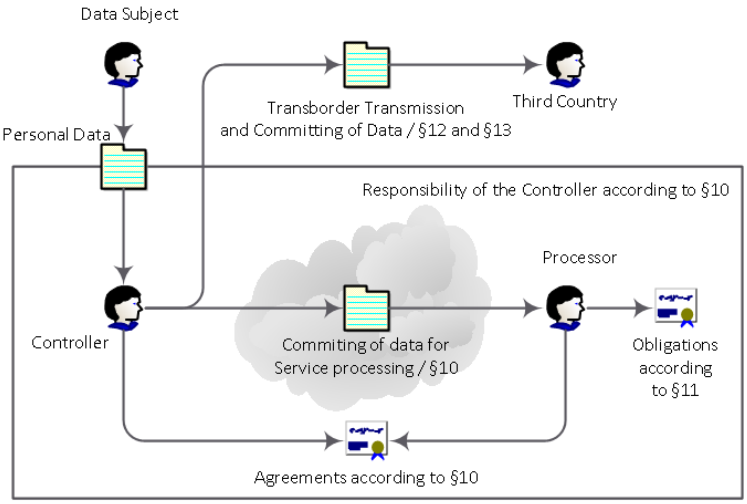

Figure 3.3: Transmission and committing of personal data according to the DSG 2000 within the context of cloud computing.

3.2.2.2 Data Transmission and Committing abroad

For the movement of data abroad, an approval from the data protection commission is necessary [Gra10, p. 47]. Therefore, it is important to make a clear distinction between

the data transmission within the EEA and beyond.

The basic requirement for every transmission or committing of data abroad to be permissible is the domestically legitimate use of data, according to §7.

Within the European Economic Area (EEA)

By the implementation of the European data protection directive, a largely uniform level for the protection of personal data exists within the EEA [Bit06, p. 11].

Generally, there is no restriction on the transfer and committing of data to a country of the EEA. In Austria, the transfer and committing of data within the EEA is subject of §12, which specifies that the transfer and committing of data to recipients within the EEA as well as the data exchange with a recipient in a third country is free of permission under the circumstance that the recipient has an adequate level of data protection.

Outside the European Economic Area (EEA) to a third country

The EU directive regulates the transfer of personal data to third countries by Article 25 and Article 26. According to these articles, the transfer of personal data into a third country is allowed if an adequate level of data protection comparable to Europe exists. That is implemented by the Austrian law by §12. As already mentioned, §12 specifies that the data exchange to a recipient of a third country is free of permission, if an adequate level of data protection exists.

The countries which can guarantee appropriate data protection are defined by the regulation of the federal chancellor.[12] The regulation includes Switzerland and Hungary.

According to the EU-Commission, countries with the safer standards are Andorra, Argentina, Australia, Canada, Switzerland, Faeroe Islands, Guernsey, State of Israel, Isle of Man, Jersey, United States, (Transfer of Air Passenger Name Record (PNR) Data and Safe Harbor principles cf. Section 2.3.1), New Zealand, Eastern Republic of Uruguay.[13] Other cases of permission free data flow are defined in §12 (3).

If none of the above described requirements is given, the transmission and committing of data in a third country needs the permission of the data protection commission.

Figure 3.4 illustrates the above described transmission and committing of data.

[12] Datenschutzangemessenheits-Verordnung (DSAV), BGBI. II Nr. 521/1999 http://www.bka.gv.at/DocView.axd?CobId=30701, last access: 03.08.2014.

[13] Commission decisions on the adequacy of the protection of personal data in third countries, http://ec.europa.eu/justice/dataprotection/document/international-transfers/adequacy/index_en.htm, last access: 03.08.2014.

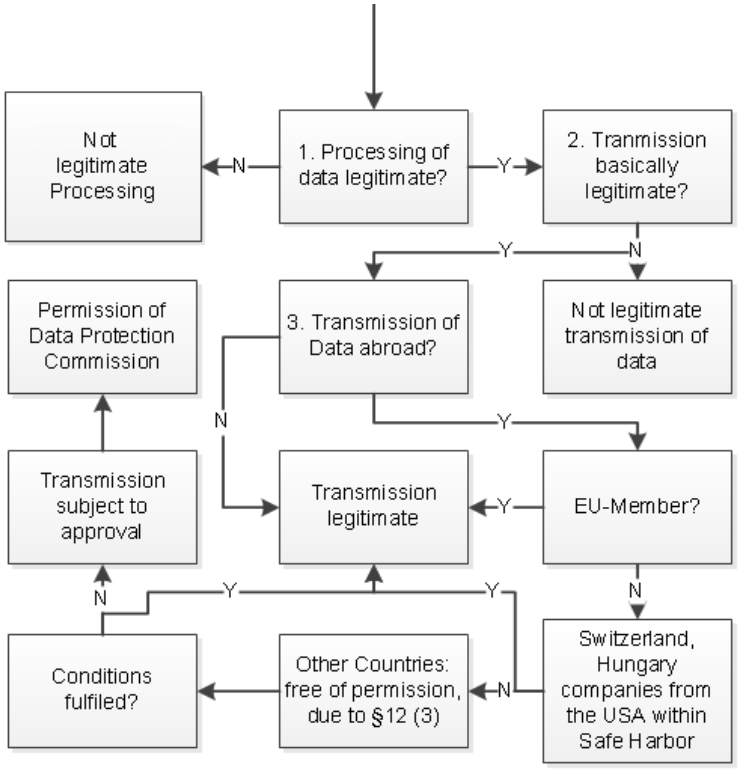

Figure 3.4: Transmission and committing of personal data adopted from [Gra10, p.50]

3.3 International Legal Compliance

So far, we discussed the legal bases of cloud computing according to Austria and the European Union. This subsection gives an overview of the legal compliance in the US.

3.3.1 Privacy Act of 1974

The *Privacy Act*[14] was the first general government law for the protection of individuals and their privacy against sovereign acts [Gen04, p. 50].

According to the US Department of Justice[15], the act focuses on four basic policy objectives:[16]

1. To restrict disclosure of personally identifiable records maintained by agencies.

[14]Privacy Act of 1974, 5 U.S.C §552a.

[15]The United States Department of Justice, http://www.justice.gov/, last access: 03.08.2014

[16]Overview of the Privacy Act of 1974, 2012 Edition, http://www.justice.gov/opcl/1974privacyact-overview.htm, last access: 03.08.2014.

2. To grant individuals increased rights of access to agency records maintained on themselves.

3. To grant individuals the right to seek amendment of agency records maintained on themselves upon a showing that the records are not accurate, relevant, timely, or complete.

4. To establish a code of "fair information practices" which requires agencies to comply with statutory norms for collection, maintenance, and dissemination of records.

3.3.2 Electronic Communications Privacy Act (ECPA)

The ECPA is defined as follows:

> "The ECPA, as amended, protects wire, oral, and electronic communications while those communications are being made, are in transit, and when they are stored on computers. The Act applies to email, telephone conversations, and data stored electronically. ECPA has three titles."[17]

The *ECPA*[18] includes a section about stored communication data. It is forbidden to access very deliberately communication devices on which data is stored temporary. Here "device" is a very broad term. From a present-day perspective, this could mean a router, switches, multiplexer, etc. Storage media used by a cloud service provider and offered as a service are also included. Moreover, it is forbidden to change the access privileges and access rules as well as to delay or prevent the access of permitted user [KT11, p. 202].

Hard penalties are the consequences, due to the following actions by [KT11, p. 202]:

- Realization of business advantages.
- Destruction and demolition of data.
- Realization of personal advantages.
- Preparation of a crime.

[17] Justice Information Sharing – US Department of Justice, Office of Justice Programs, http://it.ojp.gov/default.aspx?area=privacy&page=1285, last access: 03.08.2014.

[18] Electronic Communications Privacy Act (ECPA), 18 US.C. §2510-22.

3.3.3 Patriot Act

The US *PATRIOT Act* of 2001 modified many major US intelligence, communications, and privacy laws.[19]

The Patriot Act is about legal wire tapping. Cloud service providers are committed to pre configure so–called Intercept Access Points (IAP)[20]. Missing legal compliance will be punished. Through the Patriot Act law enforcement agencies are allowed to intercept, transmit and to process related to communication data (e.g. telephone conversations, emails or fax messages) [KT11, p. 202].

Furthermore, the Patriot Act implies security concerns for European companies. According to European lawmakers, the Patriot Act can be used to access data stored in a data warehouse in Europe. Hence, the stored data provided by a cloud service provider (US as country of domicile) could be handed over to US authorities for interception or intelligence gathering.[21]

This is one of the reasons why the European Commission started to update and revise the directive for data protection (see Chapter 3.4).

For further reading, ZDNet published a case study with the title: "How the USA PATRIOT ACT can be used to access EU data".[22]

3.3.4 Safe Harbor Principles

According to Directive 95/46/EC, the US does not have adequate legal regulations and laws for the protection of personal data which would correspond to the standard of the European Union [KT11, p. 195]. For that reason, the EU Commission and the American government agreed to accept the *Safe-Harbor-Model*, which consists of seven principles of data protection and 15 Frequently Asked Questions (FAQ) [Bit06, p. 16].

The seven Safe Harbor Principles are:[23]

- Notice - individuals must be informed about how an organization handles their data, contact information of the organization, involved third parties.
- Choice - the opportunity to opt out.
- Onward Transfer - if third parties are involved the organization must apply the notice and choice principles.

[19] Justice Information Sharing - US Department of Justice, Office of Justice Programs, http://it.ojp.gov/default.aspx?area=privacy&page=1281#contentTop , last access: 03.08.2014.

[20] IAP has the purpose of passing information to a law enforcement agency.

[21] ZDNet, http://www.zdnet.com/blog/btl/european-companies-need-confidence-over-patriot-act-concerns/56878?tag=content;siu-container, last access: 03.08.2014.

[22] ZDNet, http://www.zdnet.com/blog/igeneration/case-study-how-the-usa-patriot-act-can-be-used-to-access-eu-data/8805?tag=content;siu-container, last access: 03.08.2014.

[23] Export.gov, http://www.export.gov/safeharbor/eu/eg_main_018475.asp, last access 03.08.2014.

- Security - reasonable precautions have to be in place to prevent data loss, destruction and unauthorized access.
- Data Integrity - data has to be accurate, complete, current and relevant for the original purpose.
- Access - individuals must have the possibility to access, correct, amend or delete their personal data.
- Enforcement - procedures on a regular basis to ensure that the implemented practices are effective and sanctions in the case of violation to ensure compliance.

If an organization operating in the US agrees to the compliance of the Safe Harbor Principles and the 15 FAQs by the Federal Trade Commission (FTC)[24], then the organization has an adequate level of data protection according to the European Commission. Organizations can join Safe Harbor on voluntary basis. Companies commit themselves to comply to the principles otherwise sanctions or the stop of the data processing by the FTC would be a consequence [KT11, p. 195-196]. The list of companies joining Safe Harbor can be found under https://safeharbor.export.gov/list.aspx.

3.4 EU Data Protection Regulation - COM (2012 11)

In January 2012, the European Commission presented their proposal for a comprehensive reform of the EU's 1995 data protection rules[25]. Therefore, this subchapter gives an overview about the outlook and changes in regard to the proposed general data protection regulation. Articles important due to legal requirements and data protection companies have to consider for complying with the general data protection regulations are described more precisely in Chapter 6.

The current Data Protection Directive 95/46/EC is almost 20 years old and thus insufficient and outdated according to technological and social developments. Furthermore, the Directive is not directly applicable in the EU member states which leads to the different legislation across Europe. The new regulation would be directly applicable in every member state of the European Union.

The EU Commission started planning on 4 November 2010 to strengthen the EU data protection rules. Key goals of this approach to modernize the data protection are[26]:

- Strengthening of individuals.

[24] Federal Trade Commission, http://www.ftc.gov/, last access 03.08.2014.

[25] Commission proposes a comprehensive reform of the data protection rules, http://ec.europa.eu/justice/data-protection/news/120125_en.htm, last access: 03.08.2014

[26] European Commission, http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf, last access: 03.08.2014.

- Enhancing the single market dimension.
- Revising data protection rules in the area of police and criminal justice.
- Ensuring high levels of protection for data transferred outside the EU.
- More effective enforcement of the rules.

In 2012, the key changes of the "Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)" are as follows [Com12]:

- Single set of rules applicable across the EU.
- "Right to be forgotten": If the user no longer wants his data to be processed and the provider has no legitimate reason to keep it, the data shall be deleted.
- "Right to data portability": The user can transfer, without any problems, personal data from one service provider to another one. This is important to avoid vendor and data lock-in situations.
- Easier access to personal data.
- Clear rules on when the law of the EU applies to data controllers outside the EU.
- European data protection board. This means the introduction of a new supervisory body.
- Notification of data breaches within 24 hours: In the case data is accidentally or unlawfully destroyed, lost, altered, accessed by or disclosed to unauthorized persons, individuals and the relevant data protection authority should be notified.
- Increased responsibility and accountability for those processing personal data. This should be implemented with "privacy by design", "privacy by default", data protection risk assessments and a data protection officer for companies over 250 employees. The obligation of implementing these approaches shall be the basic setting for any IT service. Hence, data protection safeguards should be built within products and services from the earliest stage of development.
- More transparency about data handling with a better information policy is claimed.
- The right for an individual to refer all cases to their home national data protection authority is claimed.
- The rules of the general data protection regulation will also apply to organizations not established in the EU, if their services are offered in EU.

From this, it follows that the proposed general data protection regulation will strengthen the consumer's rights with changes like a single set of European rules and more data protection obligations for organizations. Once the general data protection regulation becomes effective, organizations will have to fulfill more requirements to comply with the law, especially in situations of security breaches or issues about the life cycle and the processing of data.

The general data protection regulation is longer and more comprehensive as the Directive 95/46/EC and hence, not comparable in regard to the content.

Important points of the proposal are summarized below.

Scope

The general data protection regulation has a much wider scope as the Directive 95/46/EC. The material scope states according to Article 2 that the regulation is applicable to the automated processing of personal data as well as to the non automated processing of personal data where the data is or will be stored in a file. With Article 3, the territorial scope is now extended to activities outside of the European Union. It includes any controller (also not established in the EU) which is processing personal data of an EU citizen, in the case that the processing is related to "the offering of goods or services to such data subjects in the EU, or the monitoring of their behavior".

Definitions

The basic definitions of Directive 95/46/EC are revised in the general data protection regulation. New ones are "personal data breach", "genetic data", "biometric data", "data concerning health", "main establishment", "representative", "enterprise", "group of undertakings", "binding corporate rules", and "child". Key changes are the introduction of the "personal data breach", defined as a breach of security leading to the accidental or unlawful destruction, loss, or access to personal data transmitted, stored or otherwise processed and the introduction of the "child", defined as any person below the age of 18 years.

The following definitions according to Article 4 "Definitions" of the general data protection regulation are important in respect to the presented evaluation framework within this work.

"Controller" means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes, conditions and means of the processing of personal data where the purposes, conditions and means of processing are determined by EU law or member state law, the controller or the specific criteria for his nomination may be designated by EU law or by member state law.

"Representative" means any natural or legal person established in the EU who, explicitly designated by the controller, acts and may be addressed by any supervisory authority

and other bodies in the EU instead of the controller, with regard to the obligations of the controller under this regulation.
"Processor" means a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.
"Main establishment" means as regards to the controller, the place of its establishment in the EU where the main decisions as to the purposes, conditions and means of the processing of personal data are taken; if no decisions as to the purposes, conditions and means of the processing of personal data are taken in the EU, the main establishment is the place where the main processing activities in the context of the activities of an establishment of a controller in the EU take place. As regards to the processor, 'main establishment' means the place of its central administration in the EU.
"Processing" means any operation or set of operations which is performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, erasure or destruction.

Principles

In general, the principles (Article 4) match with the Directive 95/46/EC, still some elements have been renewed or extended. Key changes in particular are the transparency principle (Article 4 (a)), the data minimization principle (Article 4 (c)) and the extension of a comprehensive responsibility and liability of the controller for processing operation. Furthermore, the principle about the processing of data is more detailed.

Rights of Data Subjects

The rights of data subjects will increase with the execution of the general data protection regulation. New rights like "Right to be forgotten and to erasure" (Article 17), "Right to data portability" (Article 18), and "Right to object" (Article 17) are introduced.

The "Right to be forgotten" allows a data subject to obtain the erasure of all the accumulated data from the controller (important particularly when social media comes into play). This is the extension of Article 12 (b) Directive 95/46/EC.

The "Right to data portability" will enable data subjects to transfer their data from one provider to another; therefore, the data subject can obtain from the controller a copy of the processed data.

Data Controller and Processor

The chapter "Controller and Processor" of the general data protection regulation clarifies the legal relationship and obligations for a controller and a processor as wells as

between them. Stated are the general obligations and requirements of the controller and processor to comply with the general data protection regulation. Many of the already existing obligations for data controllers will also apply now to processors. New obligations are:

- Controllers are obliged to implement "Data protection" by design and by default (Article 23).
- Controllers not established in the EU but where the regulation applies because of their processing activities have to designate a representative in the EU (Article25).
- Controller and processor have to maintain documentation of all processing operations (Article 28).
- Controller and the processor have to implement appropriate measures for the security of processing (Article 30).
- The controller has to notify immediately the EU data protection authority in case of a personal data breach (Article 31), at least within 24 hours. Hence, the processor has to support the controller by informing him about the data breach. In case that a data breach affects the protection of the personal data of the data subject, the controller has to inform the data subject about it (Article 32).
- Controller and the processor will have to designate a data protection officer. This applies for all public authorities and by any enterprise employing more than 250 persons (Article 35). The tasks of the data protection officer are described in Article 37.

Transfer of personal data to third countries or international organizations

The general data protection regulation will still permit the transfer of personal data to third countries or international organizations wherever an adequate level of protection exists. Therefore, safeguards like binding corporate rules, standard data protection clauses and contractual clauses are used. The general principles for the data transfer outside of the EU are described in Article 40.

European Data Protection Board

The general data protection regulation introduces a new supervisory body. This is the Data Protection Board (DPA) (Article 64), which consists of the heads of the supervisory authority of each member state. The DPA will replace Article 29 (Working Party) of the Directive 95/46/EC. Hence the DPA has to ensure the consistency and enforcement of the data protection framework.

Sanctions

The general data protection regulation includes three levels of administrative sanctions for intentional or negligent breaches with the following fines (Article 79), which shall be imposed by the supervisory authority:

1. Up to 250 000 EUR, or up to 0,5% of an enterprise annual worldwide turnover
2. Up to 500 000 EUR, or up to 1% of an enterprise annual worldwide turnover
3. Up to 1 000 000 EUR, or up to 2% of an enterprise annual worldwide turnover

Some scenarios where the highest level of fines can be imposed by the supervisory authority are:

- Processing of personal data without any or sufficient legal basis.
- Not designating a representative pursuant to Article 22.
- Failing to alert or notify a personal data breach.
- Not designating a data protection officer.

3.5 Conclusion

Although the proposed data protection regulation COM (2012 11) would bring a fundamental modernization of the data protection rules in the EU, currently the old Directive 95/46/EC serves as a basis for the applicable data protection law in all EU member states. The current level of data protection from a regulatory and law perspective and the processing of data in the European Union is insufficient and outdated.

The fact that the current data protection law is a Directive results in insufficient and inconsistent regulations and the implementation of national data protection laws in each member state. In Austria, it is the DSG 2000. In the European Union, the country of domicile principle is the reason why the national law of the controller's country of domicile (registered headquarter in an EEA state) is applicable.

The proposed regulation would help to unify the data protection rights in the EU and would bring more transparency in the use of data.

Significant improvements and changes amongst others are:

- Strengthen citizens' rights: People would get more control over their personal (e.g. right to be forgotten), easier access to own data, more transparency has to be given about how the data is handled and responsibility and accountability of providers would increase.

- Strengthen the internal market: No more unnecessary costs due to different laws and regulations and communication will take place just with one authority.
- International cooperation becomes easier, clearer defined rules, simplification of the existing rules, single set of rules, simplifying transfer of data out of the EU and European businesses will benefit from the regulation due to more trust of users.

Companies using and processing personal data should already start to consider to change their data protection policies and procedures to comply with the upcoming regulation. In consideration of the implementation, the Austrian DSG 2000 will be non-representational anymore. The regulation would override the DSG 2000 completely. Two years after introducing, the draft is now adopted by the European Parliament. Hence, the regulation is not final yet and since 2012 amendments are done. The discussion between European Parliament, Council of Ministers and Commission will continue and it remains unclear when the enforcement of the regulation will take place exactly. For the regulation to become law, the Council of Ministers has to adopt it.

CHAPTER 4

Market Analysis

This chapter provides a market overview of public cloud service offers. To get an insight of the market, the analysis includes providers from all the different service models (IaaS, SaaS, PaaS) as listed in Subsection 2.3.1. Therefore the best-known providers of each service model are presented and discussed. Described are the offered products and used interfaces. Legal aspects and security issues are not included and will be discussed in the following chapters. All the described solutions below are the current offers during the elaboration of this work. Most of the information comes from the website of the respective provider.

4.1 Amazon Web Services

Amazon Web Services LLC
P.O. Box 81226
Seattle, WA 98108-1226, USA
http://aws.amazon.com

Amazon is known as one of the biggest online retailer in the world. Hence, Amazon is dealing with a huge number of customers. To ensure the availability of their online shops during normal periods as well as during peak customer demands (e.g. strong Christmas trade), many computer centers and a lot of IT capacity are necessary. The fluctuation of capacity was the reason for the idea of renting capacity during the time with less user demands. Therefore, in 2002 Amazon launched the cloud computing platform Amazon Web Services (AWS) to provide computational power and storage. In 2006, Amazon made its infrastructure web service platform available for companies and individuals on the basis of an on-demand model.

AWS is a collection of several products and services as illustrated in Figure 4.1. Relevant ones are explained within this work.

The central part of the AWS platform builds the Amazon Elastic Compute Cloud (Amazon EC2) with the provision of re-sizable compute capacity on an on-demand basis. Amazon EC2 offers the possibility to rent a variety of virtual machines (Amazon instances). All the offered web services can be used independently or together to create an individual cloud computing platform.

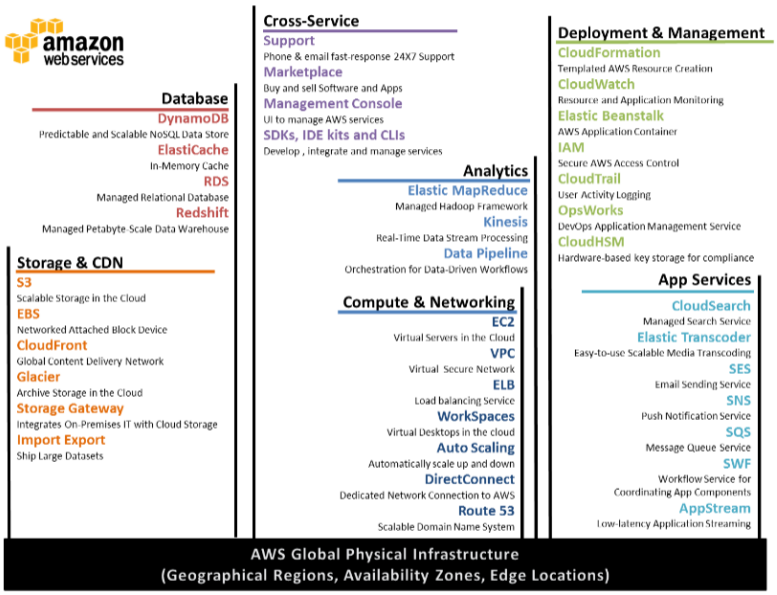

Figure 4.1: Amazon Web Services

EC2 instances can be launched in eleven different regions located around the world: US East (Virginia), US West (Oregon), US West (Northern California), EU (Ireland), EU (Frankfurt), Asia Pacific (Singapore), Asia Pacific (Tokyo), Asia Pacific (Sydney), China (Beijing), South America (Sao Paulo) and AWS GovCloud[1]. Every region is further divided into multiple *Availability Zones (AZ)*. Availability zones are distinct locations conceptually like a logical data center, completely independent and isolated from the other zones. Furthermore, availability zones have individual power, cooling, network connectivity and physical as well as network security to avoid local faultiness. Hence, failures in one specific zone will have no effect in other zones or regions. The users choose in which particular region their data and information should be stored and processed. It is also possible to deploy data in multiple zones which ensures high availability.

[1]The GovCloud is a region restricted to Federal State and local government applications, to move sensitive workloads into the cloud.

For each offered service, users pay for exactly the amount of resources needed. There are three fundamental characteristic users pay for when using AWS: compute, storage, and data transfer out. These three characteristics vary depending on the used AWS product and the selected region. The cost of data transfer is for all services the same. The inbound data transfer across all Amazon Web Services is for free as well as the outbound data transfer between services within the same region. The outbound data transfer will be summed up across the different services. Therefore, the first GB of outbound data transfer per month is for free. For up to 10 TB per month the costs are 0.120 USD per GB and with a growing transfer volume the cost will progressively increase.[2]

Amazon Elastic Compute Cloud

Amazon EC2 is a web service offer and provides resizable on-demand compute capacity (virtual servers). It gives the user the ability to launch and run virtual machines (Amazon EC2 instances) via a simple web service interface. These virtual servers are physically located in the data centers of Amazon. A random number of new server instances can be launched in a few minutes and in any availability zone. The AWS management console is illustrated in Figure 4.2.

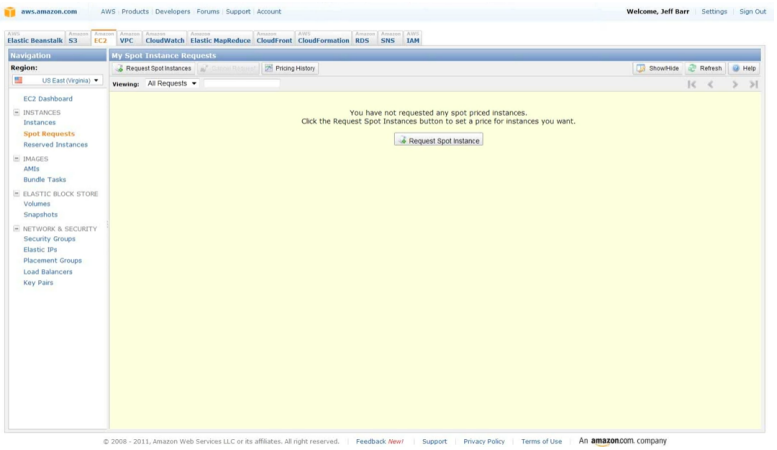

Figure 4.2: Amazon Web Services - Management Console

Amazon provides many different virtual images (called Amazon Machine Images (AMIs)) with already pre-defined operating system and pre-installed software. Hence, an AMI is a customized operating system. Additionally to the Amazon AMIs, there is a large collection of AMIs from the community. This means that every user has the

[2]Price refers to the EU (Ireland), EU (Frankfurt) and the US regions. The prices in Asia and South America are a bit higher.

possibility to install any additional tools, middleware, libraries, etc. on an AMI and to allocate it for other users[3]. An AMI is running on top of an instance. As already mentioned an instance can be launched in different zones. The name elastic refers to the ability of adding and removing instances at any time and just to pay for the used capacity.

Amazon distinguishes between various instance types which vary in their computing capacity, memory and instance storage. The smallest instance is called "micro" and the largest instance available in all regions is called "xlarge".

As already mentioned, the price varies depending on which region, operating system and instance type are purchased. Every launched instance will be charged for each started hour. Additionally, to the on-demand instances with no long-term commitment, Amazon is offering two other billing models: reserved instances and spot instances. Reserved instances are for users which can predict their demand. With a one-time payment, an instance can be reserved for a long term (1 or 3 years). In turn the cost of the hourly rate is about 50% lower. Spot instances have no fixed price for a computing hour instead the user can bid on it. Therefore, the user prepares his AMI and then bids on computing time. If the spot price is below the bid the instance will start. It automatically stops if the spot price rises above the bid. The price is based on the supply of and demand for instances and automatically determined. This model is very useful and cost-effective for applications with a flexible start and stop time. However, the reserved and spot billing models are not anymore real cloud computing offers because of the missing flexibility and elasticity.

Amazon Elastic Block Store (EBS)

Amazon Elastic Block Store is a block level storage volume for Amazon EC2 instances. An EBS volume can be attached to any EC2 instance in the same Availability Zone and as a result it can be used like a hard drive on a physical server. On an EC2 instance more than one volume with a storage size from 1 GB to 1TB can be attached. Amazon EBS volumes are independent from an instance. Thus, if an instance failure occurs it will not affect the volume. EBS also has some additional features such as the ability to create point-in-time snapshots of volumes. Summarized, EBS can be used as the primary storage for a file system, a database or other applications which require raw and unformatted block level storage. EBS General Purpose (SSD) volumes cost 0.119 USD per allocated GB per month.

Amazon Simple Storage Service (S3)

Amazon S3 is an object based and structured storage system in the cloud. The web

[3] After copying the image the user can launch as many as he wants.

services interface as illustrated in Figure 4.2 provides the possibility to store and retrieve any amount of data. Data objects up to 5 GB in size can be uploaded and will be stored in so called Amazon S3 buckets. Buckets are storage containers which serve the function of a directory and can contain an unlimited number of objects. The user has to choose in which region the bucket should be created as well as the name of the bucket. A bucket never leaves the region it was created in, except the user transfers it to another one[4]. Buckets need to have a unique name in the Amazon S3 namespace across all users. Hence, a bucket is linked with just the account which created it but can be set as public for allocation. Furthermore, each object in a bucket can be retrieved with a URL.
To access Amazon S3 buckets, the web APIs SOAP or REST-style HTTP can be used. The default download protocol is HTTP but also a BitTorrent protocol interface is provided to lower the cost for large amounts of data (high-scale) distributions.
The prices are graded according to the used TB per month. The first TB of Standard Storage per month costs 0.0324 USD per GB[5] and 0.0297 USD per GB for over 5000 TB per month. In addition, for all requests except a delete request additionally costs accrue. Another storage option is the Reduced Redundancy Storage (RSS) with a lower level of redundancy than the S3 standard storage. Amazon guarantees that the S3 standard storage is designed to provide 99.999999999% durability and 99.99% availability for objects over a given year. Furthermore, Amazon guarantees that the RRS is designed to provide 99.99% durability and 99.99% availability. The reliability is stated within the Amazon S3 Service Level Agreement. The standard storage is designed to sustain the loss of data in two facilities, the RRS is designed to sustain the loss of data in a single facility.

Amazon CloudFront

Amazon CloudFront is a web service for low latency and high speed content delivery for the Amazon Web Services products. With CloudFront either static or dynamic (e.g. streaming) content can be distributed over a global network of edge locations in Europe, US, Asia and South America. Therefore, the user has to create a download distribution with CloudFront via the web interface illustrated in Figure 4.2. The delivery mode can be either download (HTTP or HTTPS protocols are used) or streaming (RTMP protocol is used). Streaming distribution must use Amazon S3 as an origin. When serving files with CloudFront, the download distribution will detect where a request is being made and copy the file to a nearby edge location.

[4] Amazon S3 is available in all before mentioned regions.
[5] Price refers to the region EU (Frankfurt).

4.2 Salesforce.com

Salesforce.com, inc.
The Landmark @ One Market Street, Suite 300
San Francisco, CA 94105, USA
www.salesforce.com

One of the first milestones for cloud computing was the arrival of *Salesforce.com* in 1999. Salesforce pioneered the concept of delivering enterprise applications via a simple website. Today the company is the leading cloud provider of software for Customer Relationship Management (CRM).

Salesforce is offering software as a service and platform as a service. The SaaS offers are the distribution software *Sales Cloud*, the customer service software *Service Cloud*, the marketing platform *Marketing Cloud* and the community platform *Community Cloud*. Salesforce platform as a service offer is called Force.com, which can serve as a platform for the software development. Offered services by Salesforce are illustrated in Figure 4.3.

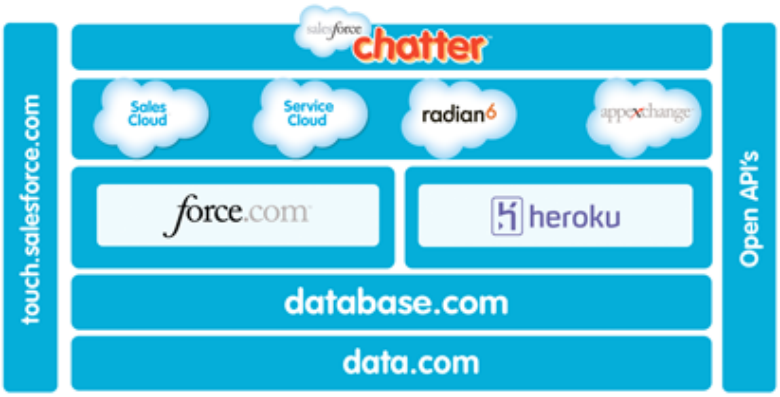

Figure 4.3: Salesforce.com Service Offers

Additionally, to the above shown services Salesforce is offering the Marketing Cloud for the automation of marketing business practices and the Community Cloud to link and share information with customers. The centerpiece of Salesforce is the Sales Cloud. It serves as a platform to optimize the sales processes in a company. The Sales Cloud should help to achieve tasks like building relationships, to close deals, and to manage distribution and marketing activities much easier. This can be achieved with a wide range of functions or cloud-based tools implemented within the Sales Cloud. With these functions, a close cooperation between marketing and sales is possible. Moreover, the Sales Cloud gives an overview of contacts and appointments as well as a comprehensive analysis of sales and forecasts. Furthermore, an interface to synchronize emails

or calendar with Microsoft Outlook or Gmail is offered. The users which need more functions can find and buy them via the service AppExchange.

In Figure 4.4, the dashboard view of the Sales Cloud is illustrated which gives the user a real-time monitoring. Each tab represents an application. Here, the applications Chatter, Contacts, Accounts, Leads, Opportunities, Files, Dashboards and Forecasts are shown. Accounts are the customers and can be connected with social media platforms like Facebook, Twitter or LinkedIn. Opportunities are the potential orders where deals could evolve out of it. The Sales Cloud like all the other offers are web-based and platform independent and can be accessed via mobile devices such as Android, iPhone, Blackberry and Windows Mobile Devices.

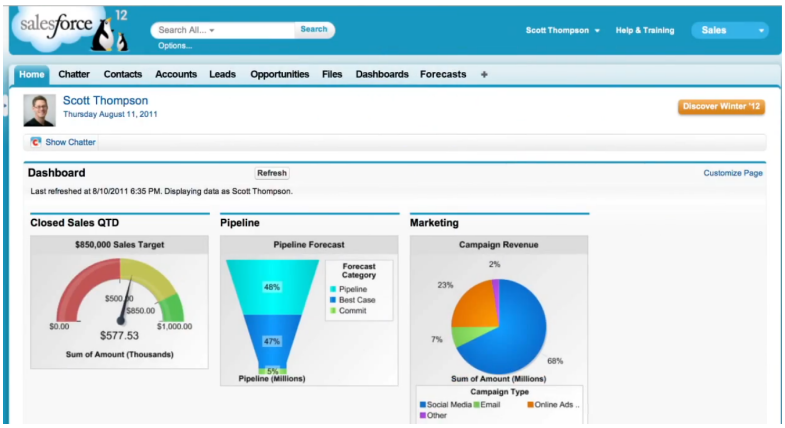

Figure 4.4: Sales Cloud - Dashboard View

The number of applications and features provided depends on the purchased Cloud edition. As of this writing Salesforce is offering for each cloud product four to five different editions. The cheapest edition for the Sales Cloud called "Group" which comes with basic sales and marketing functions costs 25 USD per month, the most expensive one is the "Unlimited" edition and costs 250 USD per month. The stated prices are just for one user.

Another software as a service offer is the Service Cloud, which serves as a platform to optimize and ease the customer service process in a company. The Service Cloud tries to combine several parts of the customer communication as well as the collaboration between agents. Therefore, traditional channels like phone, email or chat are combined with newer channels like social media communities, self-service websites and search engines. Hence, the traditional call center is supported with a number of new channels and a knowledge base. The Service Cloud is available in three different editions from 65 USD per month up to 260 USD per month. The stated prices are just for one user.

Besides, Salesforce offers the application Chatter, which serves as a "social platform" for collaboration in a company. The concept, which is very similar to Facebook

is available for the Sales Cloud and the Service Cloud. Hence, it provides the user with information about other users and groups. This helps to find experts faster and to simplify the sharing of problems and information. Chatter can be seen as a private social network with real-time information about persons and groups.

The platform as a service solution of Salesforce is called Force.com with the focus on the development of business applications. This implies that Salesforce is doing differently than other platform as a service providers. Furthermore Force.com makes the core technologies of Salesforce CRM available for the development of business applications. Therefore, Saleforce's Java based language Apex provides a set of features for building business applications. The component based framework Visualforce can be used to create interfaces using HTML, Flex and Ajax[6].

4.3 Google Cloud Platform

Google Inc. ("Google"), Amphitheatre Parkway
Mountain View, CA 94043, USA
https://cloud.google.com

Google is well known for their web search engine which was started in 1998 and their software solutions and applications. In 2014, Google combined all their cloud solutions under one name, the Google Cloud Platform, Google's portfolio of all their cloud products and services. Offered services by Google Cloud Platform are illustrated in Figure 4.5.

Figure 4.5: Google Cloud Platform

With the cloud platform Google is now also providing computational power and storage to their customer on the same infrastructure Google is hosting their applica-

[6]Further information according to programming tools and languages for Force.com are available under http://developer.force.com/.

tions. Officially Google operates twelve data centers in different regions located in North (South Carolina, Iowa, Georgia, Oklahoma, and Carolina, Oregon) and South America (Chile), Europe (Finland, Belgium and Ireland) and Asia (Taiwan and Singapore).

Compute Engine

Google's Compute Engine is the actual infrastructure as a service offer and provides re-sizable compute capacity on virtual machines which are hosted within Google's infrastructure. The concept and even the prices are more or less the same like Amazon's Elastic Compute Cloud (EC2). The Linux-based virtual machine (VM) instances can be accessed using the Compute Engine tool or command-line tool. For the location an virtual machine should be launched the customers can choose between the US and Europe.

Google Storage

Google offers three storage products: Cloud SQL, Cloud Storage, and Cloud Datastore.

The Cloud Datastore, former App Engine Datastore is a non-relational (NoSQL), schemaless data storage service where the data sets are stored as objects. A proprietary interface as well as the Java Persistence API (JPA), the Java Data Objects (JDOs), the Python datastore interface and PHP are implemented.

Google Cloud SQL provides a relational SQL database based on MySQL RDBMS. It is a web service for the administration and use of relational databases. Cloud SQL is currently available for the Google App Engine but can also be accessed via MySQL Client.

Google's Cloud Storage is a RESTful storage service for the data of an application. Google explicitly points out that non software developers should use Google Drive to store data instead.

Google App Engine

The Google App Engine (GAE) is a comprehensive platform as a service offer with a programming environment, tool support and runtime to develop and host web applications. As a runtime environment Java, Python, PHP or GO can be used, the latter two are in experimental state. With the GAE developers can focus on their web applications and do not have to care about server administration.

Applications of the GAE run in a Sandbox which allows limited access to the underlying operating system. Hence, an application cannot write to the file system. To ensure the storage of data, Google's App Engine provides the three options as described above.

Applications can be administrated with an administration console which provides full access to the public version of an application. Figure 4.6 illustrates the dashboard view of an application. The console can be used to perform basic configurations of applications, to manage cost and performance, to administrate the datastore, testing, and more.

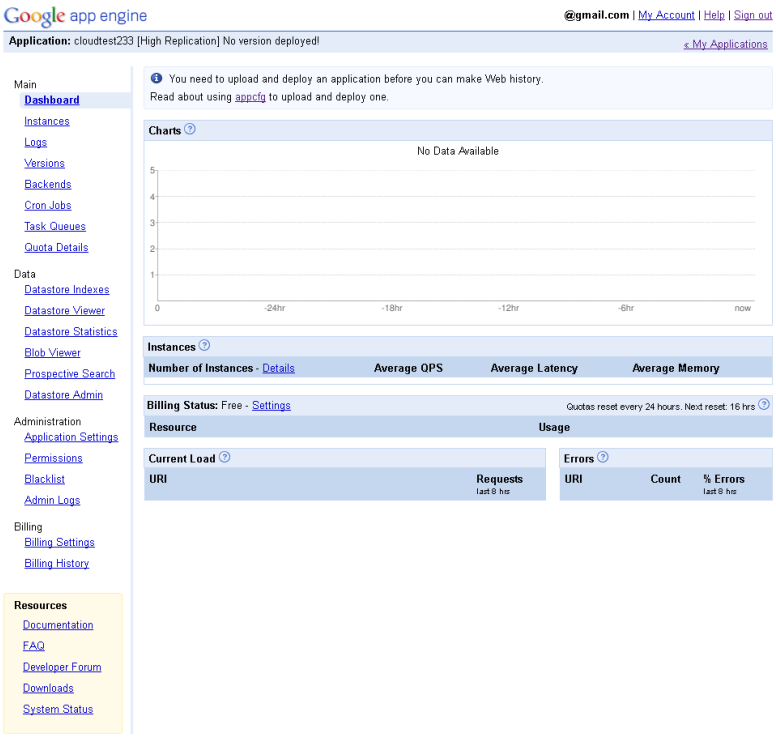

Figure 4.6: Google App Engine

The pricing of GAE is similar to the billing model of other cloud providers. Google offers a free version of the AppEngine. This includes a certain amount of computing resources for each application.

Moreover, with the Google App Engine it is not possible to choose a geographical location for the storage of data. Hence, it is not clear where the data is really stored except for the service Cloud Storage. With Cloud Storage it is possible to specify the locations of containers in the US or EU.

Google Apps

In addition to the Google Cloud Platform, Google is offering Google Apps Google's portfolio of software as a service products. It can be seen as a collection of web-based office tools. It is a customizable package of several Google products and provided as an

office suite via a web browser. For the use of Google Apps, a domain name is needed. Google Apps is intended to be used by freelancers or businesses.

Google Apps applications are:

- Communicate: Gmail, Hangout, Calendar and Google+
- Store: Drive
- Collaborate: Docs, Sheets, Forms, Slides and Sites
- Manage: Admin and Vault

All this applications can be rent to run a working environment for the daily work.

Google Apps for Work is available in 2 editions which differ in the included services and the price. The first edition costs 5 USD per month and the second one costs 10 USD per month where the second one comes with unlimited storage.

Another offer is Google Apps for Education which provides all offers like for business just for free.

4.4 Rackspace

Rackspace
5000 Walzem Road
San Antonio, TX 78218, USA
http://www.rackspace.com/

Rackspace is an IT hosting company founded 1998 in San Antonio, Texas. The main products of Rackspace are "Managed Hosting", "Cloud Hosting" and "Email & Applications". The cloud products are included in Cloud Hosting. Rackspace operates six data centers, three of them in North America (Dallas, Chicago and Northern Virgina), Europe (London), Asia (Hong Kong) and Australia (Sydney). The Rackspace Cloud offer are amongst some others divided into "Cloud Servers", "Cloud Files", "Cloud Sites" and "Cloud Load Balancer". All services can be administrated with the control panel shown in Figure 4.7.

Cloud Servers is the infrastructure as a service offer and similar to Amazon's EC2. Therewith, users can rent virtual servers (machines) with either a variety of Linux distributions or Windows. The virtualization of the machines takes place with either Xen hypervisor for Linux based instances or XenServer for Windows instances. By using Linux, each server is assigned to four virtual cores. The virtual servers can be remotely managed by the control panel or the servers API. The control panel is a web-based management interface for all cloud products and provides administrative functions for the

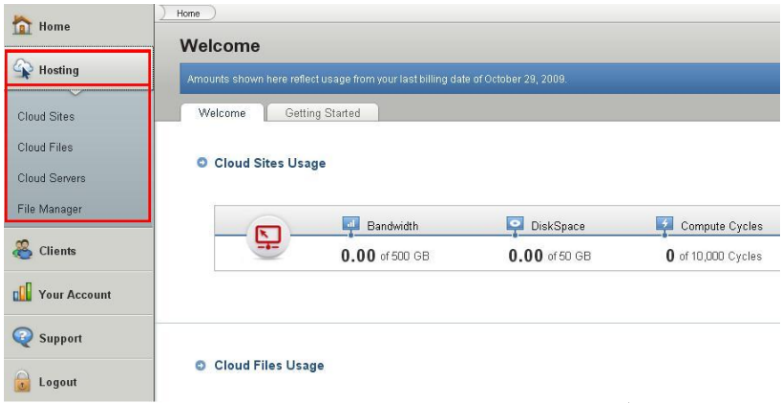

Figure 4.7: Rackspace - Controlpanel

cloud server. These functions are also available through the cloud servers' API based on a RESTful web service interface.

Furthermore, Rackspace supports SDKs in .NET, PHP, Java, Node.js, Phython and Ruby. The pricing of Rackspace is similar to the billing model of other cloud providers. The bandwidth for Cloud Servers is charged separately as also usual for an infrastructure as a service provider. Interesting for Rackspace is the guarantee of 100% availability on their data center network and power. This is unique among all cloud service providers.

Cloud Sites is Rackspace's platform as a service offer for hosting an unlimited number of websites and web applications. For each domain, Linux or Windows or even both can be used. Different technologies like Wordpress, .NETNuke, Drupal, Joomla and more can be installed on the Cloud Sites platform. Rackspace takes over the load balancing. Every page either Windows based or Linux based is served from clusters built especially for the selected operating system. Therefore, the type of the used technology will be automatically detected and each requests allocated to the most suitable pool of servers. It is interesting to note that Rackspace uses not just one but rather more servers for the hosting of applications. Typically just one server is used. The distribution of applications to more than one server comes along with some advantages such as better performance or availability. The price for Cloud Sites starts at 149 USD per month and includes 50 GB of storage, 500 GB bandwidth and 10.000 computing cycles.

Cloud Files provides scalable cloud object storage and can be used as a separate service or to extend the other services of Rackspace. Hence, it is used as an object store for Cloud Server images. It is similar to the Amazon Storage Service S3 and Amazon CloudFront. The storage space is unlimited and each file can size up to 5 gigabytes. Files can be stored in private or public data containers, latter ones can be invoked via URL and delivered by the content delivery network. Files are stored in three separated zones in a data center, where each zone has an own power supply. As with Google App Engine the specific location where the data should be stored cannot be

chosen. Files can be stored and managed via an online control panel, a desktop software or programmatically via the API. The service can be addressed by developers via a RESTful API. Additionally, frameworks such as Microsoft .NET, Java, PHP, Python and Ruby are available. Storage costs are 0.00015 USD per GB for the first TB and outgoing bandwidth 0.12 USD per GB for the first 10 TB. Incoming bandwidth and requests are for free.

4.5 Microsoft Azure

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399, USA
Azure.microsoft.com/en-us/

Microsoft Azure (Windows Azure before April 2014) is Microsoft's computing and service platform for developers available since February 2010. With Microsoft Azure, Microsoft is offering products for all types of cloud services. The services of Microsoft Azure can be used individually or together to run and manage applications (PaaS) or just by using the provided infrastructure services (IaaS). The services are a runtime environment, storage, database, messaging, identity, caching and more.

The Microsoft Azure platform includes the following products and components as illustrated in Figure 4.8. Further, development tools and the Azure Software Development Kits (templates for Visual Studio or Eclipse) can be used in a local environment (not anymore cloud computing).

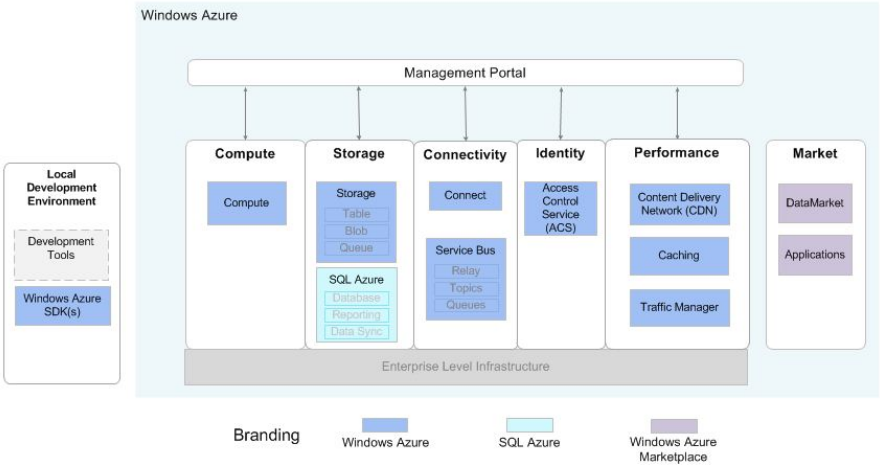

Figure 4.8: Windows Azure Platform

Microsoft's operates Azure in fourteen data centers, which are located in Asia (Hong Kong, Singapore, Saitama and Osaka), Europe (Netherlands and Ireland), United States (Illinois, Texas, Virginia, California and Iowa), South America (Sao Paulo) and Australia (New South Wales and Victoria). Microsoft states that data may be moved due to redundancy or other purposes within a geographic region (continent).

The centerpiece of the platform is Microsoft Azure Compute, which enables users to create and manage instances (virtual machines) which are isolated from other customer instances. Applications utilize resources through so called "roles" which come in three different types: cloud service role, web role and worker role. Azure recognizes which type of role is needed automatically. A role contains the code and configuration information required to carry out some part of an application's functions. Web roles provide a dedicated Internet Information Services web-server used for hosting front end web applications. A Worker Role is designed to run a variety of code (e.g. backend applications). The users can choose the location where an instance shall be executed (data center location). For the computing services Azure provides a 99.95% monthly Service Level Agreement. Costs accrue just for uses resources like for the other provider. The smallest server instance cost are 0.00135 EUR per hour and the biggest one 3.6491 EUR per hour. The rates for storage and data transfer are similar to those of Amazon Web Services.

Microsoft Azure Storage Offerings

The storage of Windows Azure can be divided into SQL data services and the second core product of the platform Microsoft Azure storage. The access works via a RESTful interface. Microsoft Azure Storage services are managed via the Azure Storage Explorer and all storage services have a 99.9% monthly SLA.

The different storage types amongst others are:

- Local Storage
- Microsoft Azure Storage
- SQL Database

The local storage comes with the Windows Azure Compute offering and provides a temporary storage for a running application instance. Hence, the storage is only accessible by the local instance. The disk space depends on the virtual machine size. Durable storage is provided with Blobs, Queues, Tables and File storage and is available as a part of the Microsoft Azure Storage Account.

Blobs (Binary Large Objects) allow the user to store large amounts of unstructured binary and text data. Tables (Indexed Record Storage) provide lightly structured storage. The Table storage is a NoSQL key-attribute data store. Queues are used for the

asynchrony communication between applications or services in Microsoft Azure and are generally based on the first in first out principle (FIFO). File storage is an NTFS file system with the usage of the Blob storage. Microsoft provides with SQL Database a relational database service.

The storage services are part of the IaaS offer by Microsoft due to the fact that it can be used inside and outside the platform.

CHAPTER 5

Security and Privacy Risks

5.1 Related Work

This section will give an overview of the related work combined and used to build the security and privacy framework within this work.

5.1.1 ENISA - Procure Secure (A guide to monitoring of security service levels in cloud contracts)[1]

ENISA (European Network and Information Security Agent) provides a practical guide aimed at the procurement and governance of cloud services with a focus on the public sector (also applicable to private sector procurement). The goal of the guide is to improve the understanding of customers about security of cloud services as well as methods used to provide an appropriate transparency during service delivery. The guide can be used as a basis for selecting between the different offerings on the market. It is addressed to users who want to understand the customer-side security aspects of cloud computing or other outsourced IT services.

A security monitoring framework in the form of a checklist and in the form of a detailed description of parameters for security monitoring is provided. According to ENISA the most relevant parameter groups which can be practically monitored are:

- Service availability. How availability is defined within the service level agreements.
- Incident response. How a service provider is responding to incidents (e.g. interruptions) and which recovery processes are in place.

[1] ENISA Procure Secure, http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/procure-secure-a-guide-to-monitoring-of-security-service-levels-in-cloud-contracts, last access: 28.09.2014.

- Service elasticity and load tolerance. How relevant resources are monitored and tested for elasticity.
- Data life-cycle management. How the service provider handles data (e.g. back-up, data loss prevention).
- Technical compliance and vulnerability management. How the service provider handles vulnerabilities and compliance with technical security policies.
- Change management. How critical changes are managed and configured.
- Data isolation. Which types of data isolation are monitored and which criteria for a failure are defined.
- Log management and forensics. Are relevant events logged and are logs reviewed and tested periodically.

These parameters serve as guidance for the continuous monitoring of security service levels and governance of outsourced cloud services. The parameters are defined and the measurement indicators are explained. This is followed by a risk profile consideration. It is determined how important each parameter could be for an organization. For each parameter, a list of monitoring and testing methodologies is provided as well as considerations for customer testing. Further, the thresholds and customer responsibilities are described. Each parameter is described in a comprehensive way with real case examples. The provided checklist guide to the document consists of question for each parameter and can be used to get an overview of risks and responsibilities.

5.1.2 Australian Government - Cloud Computing Security Consideration[2]

This paper by the Australian Government should help agencies to perform a risk assessment to determine the viability of using cloud computing services. The paper provides an overview of cloud computing and the benefits which come along with it. A checklist with questions to understand the risks related to cloud computing is provided. The authors' state that the provided questions should not be used just as a checklist but more to help to provoke a discussion about the risks. The main part of the paper is a detailed list of questions described below. The different areas contain several questions related to security which have to be considered when using cloud computing. The paper can also be used by agencies to identify and manage relevant information security risks. It can be used internally for a service provider or by the customer if the provider ensures enough transparency about the implemented security measures.

The following areas are discussed:

[2] Australian Government, http://www.asd.gov.au/publications/csocprotect/Cloud_Computing_Security_Considerations.pdf, last access: 28.09.2014.

1. Maintaining availability and business functionality. The risks and negative impacts in case that the cloud service provider becomes unavailable are highlighted within this area. It helps to understand the importance of recovery plans for the customer and provider. Therefore, the following issues are discussed: business continuity, network connectivity, disaster recovery plan, data backup, vendor availability, impact of outages, SLAs, data integrity, data restoration, and vendor lock-in.

2. Protecting data from unauthorized access by third parties. An overview of the risks related to the unauthorized access to data is provided. It helps to determine if data may be too sensitive to be used in public clouds and to be aware of the risks which come along with the storing and processing of data. Included are the choice of the deployment model, data sensitivity, legislative obligations, encryption, monitoring, data ownership, identity and access management, data location and certifications.

3. Protecting data from unauthorized access by the vendor's customers. The risks related with multi-tenancy of cloud computing are discussed within this area. It covers the issues of customer segregation, security and servers.

4. Protecting data from unauthorized access by rogue vendor employees. This topic usually comes off badly in other work about cloud computing risks. It covers the importance of the vendors' responsibilities about their employees and the administrative privileges they may have. Included are data encryption and key management in respect of how much the vendor knows. Auditing employees, physical tempering and the vendor's subcontractors are further discussed.

5. Handling security incidents. The ability of a vendor to handle security incidents is discussed within this area. Therefore, the topics support of employees, training of employees, notification and incident compensation are explained.

5.1.3 NIST - Guidelines on Security and Privacy in Public Cloud Computing[3]

This comprehensive report by NIST provides an overview of public cloud computing and some security and privacy considerations. Included topics are threats, technology risks, and safeguards related to public cloud computing environments and how to treat them. Therefore, NIST provides a list of security and privacy issues and a kind of guide for public cloud outsourcing.

The authors say that security and privacy aspects should be well thought in respect to the sensitivity of data and the responsibilities of provider and customer can change depending on the cloud service model.

[3]NIST - Guidelines on Security and Privacy in Public Cloud Computing, http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909494, last access: 28.09.2014.

Security and privacy downside of public cloud computing:

- System complexity. Many components are necessary for cloud computing which results in a larger attack surface. Further, the management of those components and the related processes to ensure efficiency becomes more complex.
- Shared multi-tenant environment. The share of components and infrastructure is unavoidable when using public clouds which results in more complex logical access security measures to prevent unauthorized access to data.
- Internet-facing services. Public cloud offers are managed via control panels or dashboards over the Internet. Therefore, risks which can arise by using the Internet have to be considered.
- Loss of control. As with other third parties, controls to ensure that organizational assets are properly protected have to be in place. Loss of control over logical and physical aspects for data and systems can also affect the legal protection for privacy.

The above described concerns lead to the following key security and privacy issues which may have long-term significance for public cloud computing. NIST describes these issues and provides precautions to mitigate them.

Governance

Governance includes the use and control of procedures, policies and standards for application development and service provisioning as well as the design, implementation, testing, use and monitoring of used services. Therefore, audit mechanisms and tools should be used to determine data handling and to verify the implementation of policies.

Compliance

Compliance deals with the different laws, regulations and standards that impose security and privacy obligations a provider and customer have to be aware of when offering or using cloud computing. Especially the topics law and regulation, data location and electronic discovery are important. Therefore, contract terms should be in accordance with the legal requirements.

Trust

The shift of data into the cloud requires a high level of trust between the customer and a provider. Therefore, insights to security and privacy controls as well as the processing of data are an advantage. This can be stated with service arrangements and clear

ownership rights over data. Further, a flexible risk management program can mitigate risks. NIST considers the following points as important for trust: insider access, data ownership, composite services, visibility, ancillary data, and risk management.

Architecture

Software and hardware for the delivery of cloud services vary among providers. Cloud providers determine physical locations and the implementation of different logics and programming interfaces. Therefore, the client has to understand the used technologies and how the provider is offering services as well as the implications on security and privacy of these technologies. The client should gather as much information as possible about the attack surface, virtual network protection and client-side protection.

Identity and access management

The protection of sensitive data and guarantee of privacy are big concerns for organizations. A cloud provider should prevent unauthorized access to data and personally identifiable information. A difficulty is to find a solution not to have two different authentication systems (internal and cloud-based). A solution therefore could be identity federation (e.g. single sign-on), which means sharing digital identities (credentials) across both domains. Moreover, identity and access management functions like authentication and access control have to be secured by adequate safeguards and should be suitable for an organization.

Software isolation

Cloud provider and customer have to understand virtualization and multi-tenancy which comes along with cloud computing and due to that the need of isolation of the customer resources.

Data protection

Organizations which move their data into the cloud must know how the access to their data is controlled and how the data is secured by the provider. Users should be aware of the fact that their data may be stored with data from other customers, which brings along risks related to data with significant concentrated value. A cloud provider should be evaluated due to the suitability of data management solutions for the data of an organization. Further, the ability to control the access to data, to secure data while at rest, in transit, and in use and to sanitize data should be evaluated. Considered should be the issues value concentration, data isolation, and data sanitization (process for removing sensitive data from storage media).

Availability

Availability means the extent of accessibility to the full computational resources of a cloud provider, which can be affected temporarily or permanently. To mitigate risks the customer should understand the contract provision and procedures for availability. Downtime and disasters are unplanned events. Hence, data backup and recovery as well as disaster recovery should fit to the continuity of an organization. The following issues should be considered: temporary outages, prolonged and permanent outages, denial of service.

Incident response

Incident response means the method of a provider in case of an attack against the computer system. Providers should have a transparent response process and sufficient mechanisms to assure a fast incident response. The response should be executed in a way that the damage is limited and the recovery time and costs are minimized. Points to consider are data availability, incident analysis and resolution.

NIST further provides a guide in respect to security and privacy issues when outsourcing data and applications to a cloud provider. It highlights the general concerns such as security and privacy issues in service contracts (inadequate policies and practices, weak confidentiality agreements, integrity and availability) and other related issues (principal-agent problem, attenuation of expertise). The principal-agent problem occurs when e.g. the cloud provider does not align the interests and business needs of the cloud customer. Three different stages of outsourcing are stated: preliminary activities, initiating and coincident activities and concluding activities. The first stage explains activities which deal with the planning and preparation of a contract. Therefore, requirements such as security, privacy must be identified before selecting a provider. Further, a service provider must be analyzed and evaluated in regard to controls of the provider's environment, level of risk and reliability. The second stage includes the overseeing of the terms in a contract. All contractual requirements should be explicitly recorded in the service agreement. The customer should be aware of the performance and the quality of the provisioned services. The third stage deals with the termination of an outsourcing contract. Therefore, important to consider are reaffirming contractual obligations, eliminating physical and electronic access rights, and recovering organizational resources and data. An exit strategy already planned within the first stage can minimize problems which can appear with the termination of a service agreement.

Summarized, the comprehensive paper by NIST helps organizations as well as providers to understand public cloud computing and the related security and privacy issues. The paper can be used by organizations to get an overview of important issues which have to be considered when deciding to outsource data into the public cloud.

5.1.4 CSA (Cloud Security Alliance) - Security Guidance for critical areas of focus in cloud computing v3.0[4]

The Cloud Security Alliance created guide which can be used by organizations to engage with cloud providers. Therefore, a set of best security practices for 13 domains divided into 2 broader categories governing and operating is provided. It is an approach for chief executives, consumers and implementers which want to adopt cloud services. For each domain, practical recommendations and requirements which can be measured and audited are described. The recommendations refer to the mitigation of risks when using cloud computing, but the authors say that due to many circumstances such as SPI model (three general accepted cloud service types as defined in Chapter 2) and different deployment models no list of security controls can cover every risk. Moreover, there is no way for a naive consumer of cloud services to completely understand what exactly he is responsible for.

In addition to the 13 domains, CSA also presents a simple framework for the evaluation of initial cloud risks and inform security decisions (quick method for evaluating the tolerance of organizations for moving an asset to various cloud computing models).

The framework allows to:

- identify the asset for the cloud deployment.
- map the asset to potential cloud deployment models.
- evaluate potential cloud service models and providers.
- map out the potential data flow.

The CSA divides the critical areas of cloud computing into two categories: governance and operations. Governance addresses strategic and policy issues, while the operational category focuses on security concerns and implementation. Below the thirteen domains are listed.

5.1.4.1 Governance

Governance and Enterprise Risk Management

This domain highlights issues related to the governance and measurement of enterprise risks. These issues are risks assessment, precedence for agreement breaches, user and provider responsibilities and the affect of international boundaries. Fundamental therefore are identification and implementation of organizational structures, processes and controls to ensure governance, risk management and compliance.

[4]CSA - Security Guidance for critical areas of focus in cloud computing v3.0, https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf, last access: 28.09.2014.

Legal Issues: Contracts and Electronic Discovery

Legal aspects and issues related to cloud computing are discussed within this domain. Issues such as protection requirements for information, security breach disclosure laws, regulatory and privacy requirements as well as international laws are specified. Specific legal issues raised by moving data to the cloud are summarized, contract considerations are listed and issues raised by e-discovery are discussed.

Compliance and Audit Management

The section provides an explanation of existing compliance and audit standards, processes and practices. Further, issues such as internal security policies and compliance requirements (regulatory, legislative and otherwise) are discussed. Compliance is defined as the awareness and adherence to obligations.

Information Management and Data Security

Managing of data in the cloud is discussed in this domain. It provides a comprehensive overview of cloud information architectures (identification and control), information management including data security lifecycle, data security controls as well as data loss prevention. Issues like responsibility, confidentiality, integrity and availability are also presented.

Interoperability and Portability

This domain discusses the issues of interoperability and portability which rise within the elastic environment of cloud computing. Interoperability is defined as requirement for the components of a cloud system to work together and should be replaceable by new components from different providers without any problems. Portability is defined as the ease of ability to move or reuse application components somewhere else. Further, recommendations for both areas and how to avoid vendor lock-in situations are provided.

5.1.4.2 Operations

Traditional Security, Business Continuity and Disaster Recovery

This domain addresses the influence of cloud computing to operational processes and procedures for the implementation of security, business continuity and disaster recovery. The possible risks of cloud computing are highlighted and the section helps to identify

security advantages and disadvantages due to cloud computing. Recommendations are given for policy, transparency, human resources, business continuity and disaster recovery.

Data Center Operations

This section discusses issues related to the data center. It should help to evaluate a data center regarding architecture and operations. CSA provides two new concepts, i.e. Cloud Application Mission and Data Center Dissemination.

Incident Response

This domain explains incident detection, response, notification and remediation to show how to enable an efficient and effective handling of security incidents. CSA describes the issues of incident handling accordingly to challenges of the different deployment models and service models to understand the complexity of incident response in the cloud. Further included are incident response lifecycle and forensic accountability.

Application Security

This domain deals with the topic of securing applications which are running on or being developed in the cloud. Further, information on how to mitigate the related risks is provided. It highlights the security influence of cloud computing over the lifetime of an application, from the design to termination. It covers the following areas: secure software development life cycle (SDLC), application security architecture in the cloud, identity and the consumption of identity as it relates to cloud application security, entitlement processes and risk-based access management as it relates to cloud encryption in cloud-based applications, application authorization management, application penetration testing for the cloud, monitoring applications in the cloud and application authentication.

Encryption and Key Management

This section discusses the issues, processes and management of encryption. Due to complexity related with encryption alternative approaches (tokenization, data anonymization, utilizing cloud database controls) are provided. Recommended are practices to protect access to resources as well as for protecting data.

Identity, Entitlement, and Access Management

CSA discusses within this domain issues related to an organization's identity when

moving into the cloud. It provides information to evaluate the readiness of an organization to use cloud-based identity, entitlement and access management (IdEA). CSA uses the Cloud Cube Model by the Jericho Forum 2.4 to explain the identity architecture for the cloud. Further topics discussed in this section are provisioning and governance of identity architecture for interfacing to identity, level of trust, provision of accounts, application design, and identity and data protection.

Virtualization

This section discuses issues and risks related to multi-tenancy in cloud computing. It highlights security issues of system and hardware virtualization. Hence, topics like hypervisor security, performance concerns, instant-on gaps, VM isolation / encryption are explained.

Security as a Service (SecaaS)

This domain addresses the topic of a standardized security framework for cloud computing providers and customers in the form of a provided service by a third party. It highlights the market place of such a service as well as the concerns and advantages. Security as a service is stated within this section as the delegation of detection, remediation and governance of security infrastructure. According to CSA, the following areas of Cloud Security as a Service will be most interesting for consumers:

- Identity Services and Access Management
- Data Loss Prevention
- Web Security
- Email Security
- Security Assessments
- Intrusion Management, Detection, and Prevention
- Security Information and Event Management
- Encryption
- Business Continuity and Disaster Recovery
- Network Security

The paper is very comprehensive and detailed especially the operational domains. It can help customers and providers to understand the importance of almost every issue related to the risks of cloud computing.

5.2 Security and Privacy Risks

Among all the benefits which come along with cloud computing many security and privacy concerns arise. Most of them are not new and can be found in any IT environment. However, due to cloud computing more security issues emerge as a result of the bigger attack surface. Virtualization, multi-tenancy, outsourcing and more features raise many questions according to how a provider runs his security policy and how he is handling security issues.

In this section, we discuss the security and privacy risks regarding public cloud computing. The most common risks are identified and described in detail.

The widely quoted survey illustrated in Figure 5.1 from 2009 by the International Data Corporation (IDC) shows the importance of security in regard to cloud computing. According to the request: "Rate the challenges/issues of the cloud on demand model", the issues security, availability and performance have taken the front places. 87,5% of the sample are very concerned about security. For comparison, the issue availability took the second place with 83,3%.

Securing data in the cloud is not only the responsibility of the service provider, also the customer has to take care of his data as good as possible. The level of accountability and responsibility depends on which cloud service model is used. The service types differ in regard to security responsibilities for user and provider. In a SaaS environment, the implementation of security measures is more the responsibility of the provider. Security and privacy issues should be defined legally within a contract. In an IaaS environment, the provider is responsible for securing the infrastructure, securing the installed software is the responsibility of the user. PaaS is in between, the provider is responsible for securing the platform and infrastructure but for the application security the user is responsible. In summary, going down the stack of service models means less responsibility for the provider and on the other hand more responsibility for the user in respect of security and privacy prevention [All11, p. 22]. An organization should make a contract with the provider to ensure the compliance with laws and regulations; this does not depend on the chosen service model.

In 2008, Gartner announced seven cloud computing security risks users have to face with when using cloud computing, which are relevant until today:

1. Privileged user access
2. Regulatory compliance
3. Data location
4. Data segregation

[5] International Data Corporation - Cloud Challenges/Issues Survey, http://blogs.idc.com/ie/wp-content/uploads/2009/12/idc_cloud_challenges_2009.jpg, last access 19.04.2012.

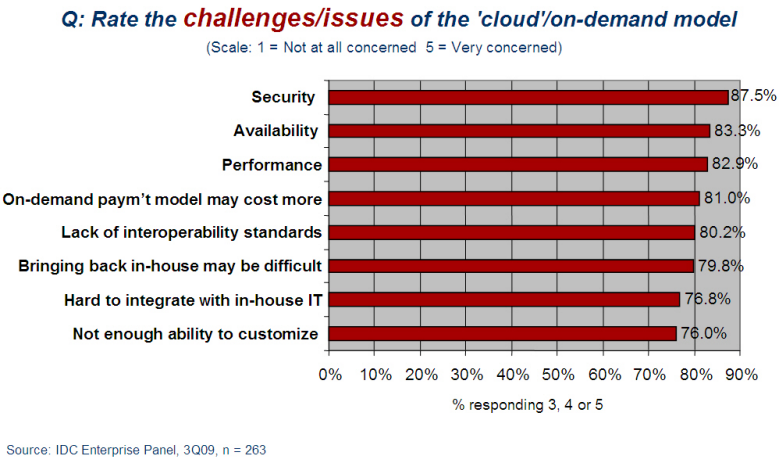

Figure 5.1: Survey by the International Data Corporation (IDC)[5]

5. Recovery
6. Investigative support
7. Long-term viability

According to NIST, the key issues of cloud computing are:

- trust,
- multi-tenancy,
- encryption,
- compliance.

The following paragraphs give an overview of the risks and areas of concern which arise when using cloud computing. The thirteen listed risks do not follow any order and are all important for the further work of this thesis.

Loss of Control / Loss of Governance

Common for cloud computing is the transfer of responsibility, control of information and components to the cloud provider, which makes the customer depending of the provider. This loss of control includes the reduction of maintaining security and privacy decisions for the provider [WJ11, p. 12]. The loss of control can have a critical impact on the strategies and goals for an organization and can make the complying with security requirements or laws difficult. Further, if a provider outsources its services to third

parties or the terms and conditions change, the services may not be provided anymore in a lawful way [ENI09, p. 29].

Vendor Lock-in

Vendor lock-in means that the provider locks in the customer to the vendor's wares. The lock-in is, for-example, linked to the application programming interfaces (APIs) of the used cloud. Without any standardization users are not able to easily move their programs from one provider to another. Hence, limited freedom of action and increased costs for customers emerge [Cho11, p. 129]. Further, not just the moving of data and applications between different providers also the migration back to an in-house IT environment may become impossible [ENI09, p. 22].

Data - Software Isolation / Data Segregation

Data can be the application programs, scripts, settings, records and account information about the users of the applications. With access controls it is possible to protect data from unauthorized users but encryption is also an important point. Isolation becomes important due to multi-tenancy and physically shared resources such as storage and capacity between different customers in an IaaS cloud environment [ENI09, p. 35]. The components which realize this infrastructure and virtualization were not designed for a strong isolation, that could lead to the risk that users may have access to any other tenant's data [All10, p. 11]. Hence, the isolation of data and software is dealing with the discrete access to a shared pool of resources by legitimate users and should be taken as an essential risk especially when using sensitive data [GH12, p. 42]. A clean segregation of data and applications for every customer must be guaranteed by a cloud provider. If the physical control of data is missing encryption is the only way of securing data [LB11, p. 30].

Data Location

Data location is a common compliance issue of cloud computing. A company which is using an in-house data or computing center always knows where their data is stored, how the data will be processed and how the data are protected. A characteristic of cloud computing is that data are stored redundantly in several data centers around the world. Sometimes information about the data location as well as used safeguards is unavailable for the customer. Hence, that makes it difficult for customers to know if legal and regulatory compliance requirements are fulfilled. Further, the cross boarder processing of data rises many concerns in regard to the applicable law [WJ11, p. 17]. The knowledge of the location of stored and processed data is essential for customers to be aware of which law is applicable.

Privileged User Access / Malicious Insider / Insider Access

Data stored on a cloud provider's server means that the circle of insiders expands. This security handover outside the physical boundaries of an organization leads to an inherent level of risk [WJ11, p. 18]. Depending on the level of access of malicious insider the impact they can have on an organization is considerable [All10, p. 10]. According to [ENI09, p. 36] activities of malicious insiders can have impact on

> "the confidentiality, integrity and availability of all kind of data, IP, all kind of services and therefore indirectly on the organization's reputation, customer trust and the experiences of employees."

Hence, it is important to collect as much information as possible about who is managing the data as well as privileged administrators and the control over their access.

Regulatory Compliance / Compliance Risks (CSA)

Regulatory compliance coheres with the reliability of a provider. A cloud provider is responsibly to comply with laws, regulation, standards and specifications [WJ11, p. 15]. Some of these laws and regulation are further described in Section 3. The risks are that a cloud provider may not fulfill these requirements or does not permit audit by the customer or third parties [ENI09, p. 30].

Incident Response

Incident response means the method of the provider to deal with the consequences of an attack against the security of a computer system. This includes incident verification, attack analysis, containment, data collection and preservation, problem remediation and service restoration. The response of a provider should be provided in a way that limits the damage. The process and mechanisms of the incident response should be provided in a transparent way to the customers [WJ11, p. 33]. If providers do not provide enough information about their incident response plan it is a high risk for their customers.

Investigative Support / Monitoring

A cloud environment is not static and always evolves and changes. Hence, the investigation of activities is difficult. Without a periodic monitoring and testing of the services the required privacy and security standards or legislative obligations may not be fulfilled [All11, p. 38].

Disaster Recovery / Data Back-up

Cloud providers need a comprehensive disaster recovery plan. Disasters can be natural or man-made. Anyway, a provider has to implement disaster recovery solutions for the required services [All11, p. 186]. Therefore, cloud providers should replicate the data and applications infrastructure across multiple data center and zones.

Data Deletion

Insecure, incomplete or ineffective data deletion can be a high risk in the case of multiple tenancies and the reuse of hardware resources. Full data deletion is basically possible by destroying a disk but the disk maybe also stores data from other users, so it will not be destroyed immediately after the user requested it. Further, data may be available over the specified lifetime in policies. An effective way of encryption may lower the level of risks [ENI09, p. 40].

Data Loss / Leakage

Data loss includes the topics of identity and access management, encryption and key management, and information lifecycle management. Data loss can be the result of insufficient authentication, authorization and audit (AAA) controls, inconsistent use of encryption and software keys, operational failures, persistence and remanence challenges, disposal challenges, risk of association, jurisdiction and political issues, data center reliability and disaster recovery. Data must be protected from unauthorized access by third parties since due to the characteristics of a cloud environment the threat of data compromise increases. The impact of data loss or data leakage can be fatal for an organization's business [All10, p. 12].

Business Continuity / Availability / Outages

A vendor should provide a business continuity plan. Important is that the SLA provides a guarantee that the provider offers adequate system availability and quality of service. A customer should know which impact an outage can have and if he can tolerate the maximum possible downtime of the SLA. In general, SLAs guarantee 99.9% availability but that also means up to nine hours of unscheduled outages every year, without breaking the SLA [oD11, p. 9]. Moreover, the service agreement should be clear about what is meant by availability and how it will be monitored [GH12, p. 14]. In the case the service provider goes bankrupt it is important that the data will still remain available. Business functionality can be a negative impact if the vendor's cloud service becomes unavailable, especially if critical data has been moved to the cloud. Further, a cloud provider has to ensure an appropriate availability for their customers. It

is an advantage when the customer can review the business continuity plans and disaster recovery plans. This should be captured within a contract to ensure that appropriate compensation is considered [NA10, p. 253]. Due to the competitive market it is also possible that provider's have to restructure their service portfolio which could lead to the termination of services. That, can also have serious impact on the business continuity of the provider such as quality of service or a loss of investment. Moreover, failures and outages of the provider can cause problems for the customer to meet the obligations to its own customers [ENI09, p. 31].

A cloud customer should always be aware of the impact a significant outage can have, sometimes SLAs may not be enough [All11, p. 75].

Security

Many of the above described risks also deal with security. This describes the risks related with the data transfer, interfaces and APIs. Security issues amongst others can be: anonymous access or inflexible access controls, reusable passwords, transmission of content, clear text authentication or improper authentication, limited monitoring and unknown services [All10, p. 9].

However, many of the listed issues deal with the protection of data. Hence, due to the loss of control when using cloud infrastructure from a provider the protection of data gets top priority. As a consequence, mechanisms to secure the storage and processing of data to provide risk mitigation must be provided as well as an investment in comply with regulations, certifications and audits.

CHAPTER 6

Frameworks

6.1 Evaluation Framework

The framework, as illustrated in Figure 6.1, provides requirements which should be considered if organizations or persons decide to use cloud computing. The framework should help to decide if a cloud provider can be assumed to be reliable. The areas of relevance are based on the provided information from widely accepted institutions as described before in this work. We can deduce therefore that in general the areas of concern can be divided into legal and technical issues and requirements. In both areas, data protection is a big issue. The used terms in the framework are defined in the previous sections.

6.1.1 Scope and Structure

The framework can be used as a guide or checklist to figure out if cloud providers fulfill different standards and requirements. Further, the framework can serve providers as a guide to identify weaknesses and strengths of their offered services. The framework helps customers to decide if a cloud provider can be assumed as reliable. Moreover, the framework highlights the responsibilities for both the provider and the user.

The framework is divided in two main areas of requirements:

1. Legal and organizational requirements

2. Data protection and technical requirements

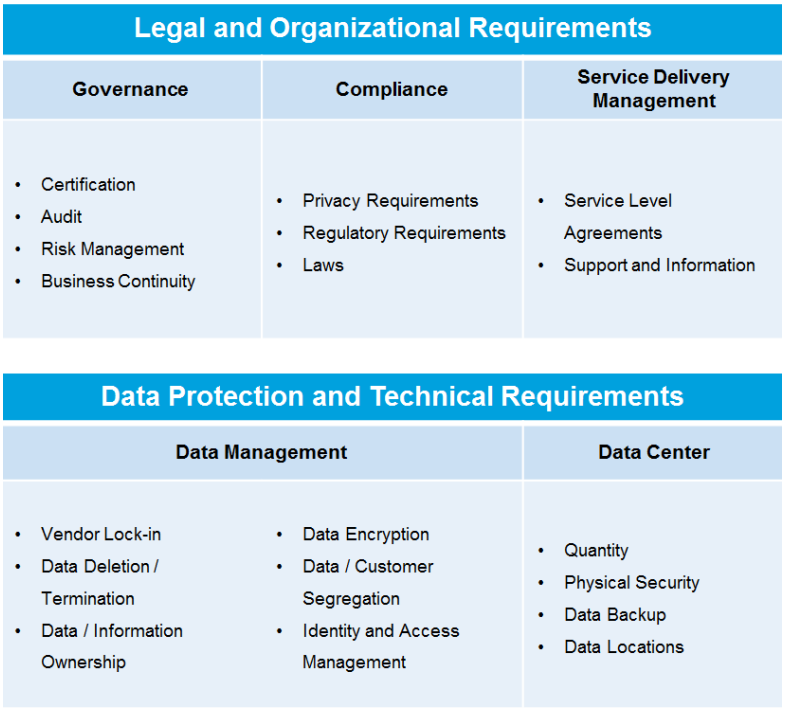

Figure 6.1: Evaluation Framework

Evaluation Levels

The result of the evaluation is based on three fulfillment levels. Depending on the degree to which the different requirements (Figure 6.1) as described in detail below are fulfilled the rating will be weak, average or strong.

Level of fulfillment:

- Weak
  The requirements are not fulfilled and/or documentation about the specific area is non-existing.

- Average
  The requirements are fulfilled and documentation about the specific area is provided. The requirements are addressed with room for improvement.

- Strong
  The requirements are completely fulfilled and large quantity of extensive documentation is available. Processes and documentation is adapted regularly and the provider has differentiated itself of the others.

As shown in the framework, both areas of requirements are further divided into several categories, which are described in detail below.

6.1.1.1 Legal and Organizational Requirements

Legal and organizational requirements include the topics governance, compliance and service delivery management. All these areas are related to the question how trustful and reliable a service provider acts according to organizational policies, laws, regulations and standards.

A service provider should possess the following points to fulfill legal and organizational requirements.

Governance

Governance includes the accountability, responsibility and transparency of an organization. Formalized processes and procedures based on compliance requirements with IT standards and regulations must be implemented. Certifications and audits help to enhance trust because users are not able to get a complete insight of all security relevant issues and implemented controls. Hence, the provider should offer information about certifications received and audits executed. Third party audits should be a vital part of any assurance program.

To ensure the continuing suitability, adequacy and effectiveness of security, risks and compliance programs, formalized processes for security governance and risk management have to be implemented. Further, business continuity management to guaranty the continuity of services has to be in place.

Compliance

Compliance to laws, regulations and other regulatory authorities is the base for every service provider to become reliable and must be adequately met. It refers to an organization's responsibility to comply with regulations, laws and standards to assure secure services. Audits demonstrate that a common standard of security and governance is reached. Contractual obligations to protect personal information are essential to mitigate security and privacy risks. Users should be aware of the fact that laws and regulations can change depending on where the data is stored and processed. Therefore, a reliable cloud provider should identify and know cross-border data transfer issues and if possible mitigate them.

Legislative obligations and audit standards as discussed in Chapter 3 are:

- Federal Information Security Management Act (FISMA). FISMA is a US federal law to provide integrity and confidentially to information by strengthening infor-

mation security.[1]

- Sarbanes-Oxley Act (SOX). SOX is a US federal law implemented to protect shareholders and investors of fraudulent activities related to the account of an enterprise with the improvement of financial disclosures. This can be done by implementing internal control standards and frameworks (e.g. COSO).[2]
- Safe Harbor Framework. Seven principals of data protection for an adequate level of data protection according to the European Commision.[3]
- Statement on Standards for Attestation No. 16 (SSAE 16). SSAE 16 replaced the former SAS70 as a guide for reporting on service organizations.[4]
- EU Data Protection Directive 95/46/EC. Reference text and basis for the protection law and regulations of personal data in the EU.[5]
- ISO/IEC 27001 Information Security Management. A standard to secure information security.[6]

Service Delivery Management

Managing service levels and providing effective customer support is essential and only possible if effective service delivery processes are in place. Therefore, formal service level agreements and terms of service must be available. A SLA should at least contain the requirements according to the business needs, relevant national and international standards, clearly defined security requirements for both parties, levels of support, system availability (e.g. uptime, response time), compensation in case of a breach (e.g. data loss) and measures in case of failure or critical situations. Without adequate SLAs there is a risk that the provision of systems, services and support by the provider do not meet users' expectations.

A cloud provider should make available to their users as much information as possible. Therefore, support and information are necessary. This further includes formalized and implemented structured processes for the handling of incident management and performance/capacity management.

The following information and support should be available to users:

[1] FISMA, http://csrc.nist.gov/groups/SMA/fisma/, last access: 12.10.2014.

[2] SOX, http://www.sec.gov/about/laws.shtml#sox2002, last access: 12.10.2014.

[3] http://www.export.gov/safeharbor/, last access: 12.10.2014.

[4] SSAE16, http://ssae16.com/, last access: 12.10.2014.

[5] European Parliament and Council Directive 95/46/EC 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 [Official Journal L 281 of 23.11.1995].

[6] ISO/IEC 27001, http://www.iso.org/iso/home/standards/management-standards/iso27001.htm, last access: 12.10.2014.

- Frequently Ask Questions (FAQ)
- Help Lines, wikis and forums
- Documentation about security
- Information about the billing system

6.1.1.2 Data Protection and Technical Requirements

The protection of data is a vital issue to make a cloud environment secure. Data protection and technical requirements include the topics data life cycle, data center, privacy and security management. A service provider should possess the following points to fulfill data and information protection requirements.

Data Management

Formalized processes and procedures for the integrity and management of data and information have to be in place. Measures to prevent the misuse of data, data loss and unauthorized access must be implemented.

The following points related to data management should be considered:

- Vendor Lock-in. For users, it is essential to know if it is possible to export their data and applications to other providers or back to their own IT-environment. Exit strategies and other options should be stated in a contract.
- Data Deletion / Termination. For a cloud customer it is important to know, if and how data are deleted, to prevent that the provider continuously stores data even after service termination. A formal process for the secure disposal of information as well as storage media should be in place. Further, all data should be securely deleted from shared hardware resources.
- Data / Information Ownership. It should be clear who possesses information and data and who is responsible for them. Hence, information about the data ownership should be stated in an agreement to avoid security breaches for critical information.
- Data Encryption. Encryption techniques, software and key management should be implemented. Information about encryption should be provided.
- Data / Customer Segregation. Personal data about customers should be segregated and access limited to mitigate the related risks.

- Identity and Access Management. Access to appropriate levels of data should be managed. Proper processes and security mechanisms to avoid unauthorized access to information and data (e.g. access control, authentication and authorization management) have to be implemented.

Data Center

A high standard of protection requires the access to information in data centers and the mechanisms that are used to secure a data center (physical security).

The following points about data centers should be considered:

- Quantity. Information about how many data centers are used to store and process data should be available. The number of data centers increases the security of data and information.
- Physical Security. Information about the physical provisions to secure the data centers should exist. This also includes who has physical access to the data center and infrastructure.
- Data Backup. It should be possible to backup and store data in several locations. The user should get the information of automated back-up and restore plans.
- Data Location. Information about the location of the data centers should be provided. At best, the user can choose where his data will be stored.

6.2 Evaluation

In this section the results of the cloud provider evaluation are described.

6.2.1 Amazon AWS

Amazon Web Services is one of the big players and leaders as cloud service provider, especially for the infrastructure as a service model. For further details about AWS please refer to Chapter 4.

Legal and Organizational Requirements

Figure 6.2 shows the results of the evaluation for legal and organizational requirements.

Governance
Amazon addresses the topics accountability, responsibility and transparency very comprehensive. With the AWS Security Center and AWS Compliance an extensive amount of documentation (e.g. whitepaper, programs, and certifications) is provided. Amazon

provides their customers auditing security checklists for the use of AWS. Formalized risk management and IT governance processes and programs are defined.

Compliance
Within the AWS Compliance platform Amazon provides their third party attestations, reports and certifications. Further, Amazon states in detail assurance programs and compliance initiatives. Amazon is certified with the common practices.

Service Delivery Management
Several channels for customer support are offered. Information and support is made available to the customer with the common standards. A general customer agreement is in place, as well as specific service level agreements for each of the provided services. An adequate compensation in case of a security breach was not found during the evaluation.

Figure 6.2: Legal and Organizational Requirements - Amazon Web Services

Data Protection and Technical Requirements

Documentation about relevant security measures to protect customer information and data is available. Figure 6.3 shows the results of the evaluation for data protection and security requirements.

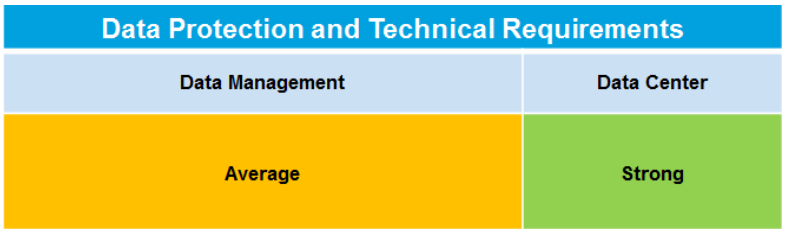

Figure 6.3: Data Protection and Technical Requirements - Amazon Web Services

Data Management Requirements

- Vendor Lock-in - Average
  Amazon states in its service terms that during a migration of data Amazon is not responsible for any damage or loss incurred during the shipment. Amazon offers the AWS Import/Export service to transfer data in and out of the AWS cloud.
- Data Deletion - Weak
  No information about data deletion / termination was found during the evaluation.
- Data / Information Ownership - Strong
  The ownership is clearly defined in agreements and explained within white papers.
- Data Encryption - Strong
  Encryption techniques and used software are extensively described.
- Data / Customer Segregation - Average
  Segregation is achieved with the implementation of the security management processes. Documentation is partly available.
- Identity and Access Management - Strong
  Processes and extensive documentation are available.

Data Center Requirements

- Quantity - Strong
  An adequate number of data centers is in place, users can choose to store their data and information between the different locations. Documentation is available.
- Physical Security - Strong
  Extensive documentation and certifications for physical security are in place.
- Data Backup - Strong
  Automated backups and DB snapshots are implemented and documented.
- Data Location- Strong
  Data locations are known and the user can choose where the information and data should be stored.

6.2.2 Google Cloud Platform

With the Google Cloud Platform, Google offers computing power, storage and the platform as a service product App Engine. For further details about Google please refer to Chapter 4.

Legal and Organizational Requirements

Figure 6.4 shows the results of the evaluation for legal and organizational requirements.

Governance
Google's approach on governance is compared to other providers weak. Google does provide little documentation about governance, compliance and risk management plans and strategies. No complete and formalized risk management or IT governance processes were found during the evaluation. Hence, a lack of documentation for the area governance was observed.

Compliance
Google is certified with the common practices. Documentation and initiatives are partly in place.

Service Delivery Management
Customer support in the way of FAQs, forums and help lines exists. Further technical documentation for the specific services is developed but partly in place for the topic security. General terms of service are in place and for the specific services adequate service level agreements exist. An adequate compensation in case of a security breach was not found during the evaluation.

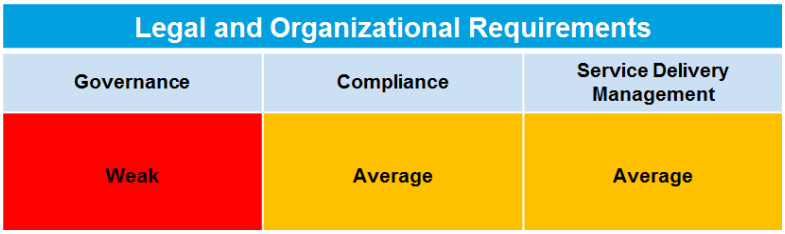

Figure 6.4: Legal and Organizational Requirements - Google Cloud Platform

Data Protection and Technical Requirements

Documentation about relevant security measures to protect customer information and data is partly available. Figure 6.5 shows the results of the evaluation for data protection and security requirements.

Data Management Requirements

- Vendor Lock-in - Weak
  Documentation about the handling of data migrations exists.

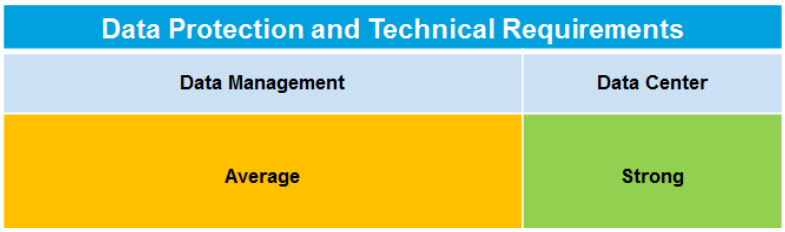

Figure 6.5: Data Protection and Technical Requirements - Google Cloud Platform

- Data Deletion - Weak
  No information about data deletion / termination was found during the evaluation.
- Data / Information Ownership - Weak
  The ownership of assets is partly defined.
- Data Encryption - Average
  Encryption techniques and used software are in place and documented.
- Data / Customer Segregation - Average
  Segregation is achieved with the implementation of security management processes. Documentation is partly available.
- Identity and Access Management - Average
  Documentation is available.

Data Center Requirements

- Quantity - Strong
  An adequate number of data centers is in place.
- Physical Security - Average
  Little documentation about physical security exists.
- Data Backup - Average
  Automated backups are implemented and partly documented.
- Data Location- Strong
  Data locations are known and the user can choose where the information and data should be stored.

6.2.3 Salesforce.com

Salesforce offers software as a service and platform as a service products. Salesforce with the platform Force.com became one of the big players as a cloud provider for the

service model platform as a service. For further details about Salesforce please refer to Chapter 4.

Legal and Organizational Requirements

Figure 6.6 shows the results of the evaluation for legal and organizational requirements.

Governance
Salesforce provides information and documentation about governance, certifications, governance cooperation and programs within the trust and compliance documentation. A lack of formalized processes and documentation about business continuity and risk management was observed during the evaluation.

Compliance
Salesforce provides their third party attestations, reports and certifications and complies with the common standards.

Service Delivery Management
The common standards and good practices are used for the support of customers. Information and documentation for customers are available via the Salesforce website. Master subscription agreement as well as specific agreements and terms for the respective services are available.

Legal and Organizational Requirements		
Governance	Compliance	Service Delivery Management
Average	Average	Average

Figure 6.6: Legal and Organizational Requirements - Salesforce

Data Protection and Technical Requirements

Documentation about relevant security measures to protect customer information and data is available. Figure 6.7 shows the results of the evaluation for data protection and security requirements.

Data Management Requirements

- Vendor Lock-in - Average
  Documentation about data migration procedures are available. The responsibilities for data migrations are stated within the contractual relationship.
- Data Deletion - Strong
  Documentation is available and data deletion is explicitly stated in the service contracts.
- Data / Information Ownership - Strong
  The responsibilities of information ownership is clearly defined.
- Data Encryption - Strong
  Encryption techniques and used software are in place and documentation is extensively available.
- Data / Customer Segregation - Average
  Data and Customer segregation are implemented, documentation is partly available.
- Identity and Access Management - Weak
  Documentation is partly available.

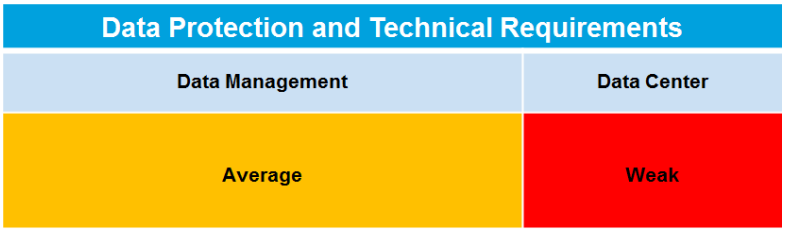

Figure 6.7: Data Protection and Technical Requirements - Salesforce

Data Center Requirements

- Quantity - Average
  An adequate number of data centers are in place. Documentation is partly available.
- Physical Security - Average
  Documentation and certifications for physical security are partly available.
- Data Backup - Average
  Automated backups are implemented and documentation is partly available.
- Data Location- Weak
  Data locations are partly provided to the customer.

6.2.4 Microsoft Azure

Azure is Microsoft's computing and service platform. For further details about Microsoft Azure please refer to Chapter 4.

Legal and Organizational Requirements

Figure 6.8 shows the results of the evaluation for legal and organizational requirements.

Governance
Microsoft is offering extensive documentation about governance, compliance, audits and risk management. Assurance programs, cooperation's and documentation about IT governance policies exist.

Compliance
Microsoft is certified with the common practices. Documentation, initiatives and cooperation with third parties exists.

Service Delivery Management
Customer Support and well defined service level agreements are available. An adequate compensation in case of a security breach was not found during the evaluation.

Legal and Organizational Requirements		
Governance	Compliance	Service Delivery Management
Strong	Strong	Average

Figure 6.8: Legal and Organizational Requirements - Microsoft Azure

Data Protection and Technical Requirements

Documentation about relevant security measures to protect customer information and data is available. Figure 6.9 shows the results of the evaluation for data protection and security requirements.

Data Management Requirements

- Vendor Lock-in - Weak
  Documentation about data migration exists.

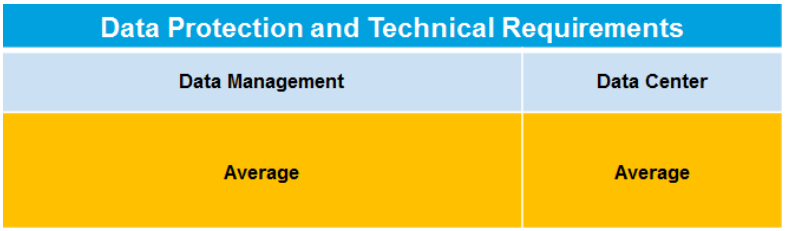

Figure 6.9: Data Protection and Technical Requirements - Microsoft Azure

- Data Deletion - Weak
  No information about data deletion / termination was found during the evaluation.
- Data / Information Ownership - Average
  The ownership of assets is clearly defined.
- Data Encryption - Average
  Encryption techniques and used software are in place and documented.
- Data / Customer Segregation - Average
  Segregation is achieved with the implementation of security management processes. Documentation is partly available.
- Identity and Access Management - Average
  Documentation is available.

Data Center Requirements

- Quantity - Strong
  An adequate number of data centers is in place.
- Physical Security - Average
  Documentation about physical security exists.
- Data Backup - Average
  Automated backups are implemented and partly documented.
- Data Location- Average
  Data locations are known. Microsoft states users may choose where the information and data should be stored.

6.3 Summary

The following Figure 6.10 shows the results of the evaluation.

Provider	Legal and Organizational Requirements			Data Protection and Technical Requirements	
	Governance	Compliance	Service Delivery Management	Data Management	Data Center
Amazon AWS	Strong	Strong	Average	Average	Strong
Google Cloud Platform	Weak	Average	Average	Average	Strong
Salesforce	Average	Average	Average	Average	Weak
Microsoft Azure	Strong	Strong	Average	Average	Average

Figure 6.10: Evaluation Summary

A lack of transparency and missing documentation makes it difficult for organizations and users to understand the related risks which come with cloud computing and the complex environment. Formalized processes and controls for IT governance and compliance must be implemented and documentation has to be available to help users identifying, if the aims and related risks are in accordance with their business strategies and needs. The evaluation shows that Microsoft and Amazon completely fulfill these requirements, especially Amazon which provides an extensive amount of documentation to their customers. On the other side, Figure 6.10 illustrates that Google has a backlog in governance requirements compared to the other evaluated providers. The compliance with laws, regulations and other regulatory requirements is proved by implementing good practices and certifications. The difference between the providers, in this area is the amount and quality of information and documentation provided. Further, Microsoft and Amazon work together with institutes and regulations to help improving standards and certifications. Service delivery management is equally pronounced for all four providers. Support, FAQs, Wiki, etc. are in place by all evaluated providers, they differ in the way and form they are arranged. SLAs are in place for all services. During the evaluation, an adequate compensation in case of a security breach was not found for any of the evaluated providers. According to security and privacy of information and data (data management) all evaluated providers are more or less on the same level. Interesting are the results for vendor lock-in and data deletion. We can state that climbing up the stack of service models (IaaS, PaaS, SaaS) it becomes more difficult to migrate data from one provider to another provider. Hence for SaaS and PaaS the vendor lock-in is stronger due to technical issues as for an IaaS offer. Data deletion and termination after ending the cooperation are addressed in a weak way by all providers, except Salesforce. The other providers do not state data deletion in their documentation or agreements. For the physical protection of data and data centers, it can be assumed that an acceptable amount of data centers and controls are in place. Anyway, the possibility of storing data

in different regions and amount of documentation provided lead to the different ratings as illustrated in Figure 6.10.

6.4 EU Data Protection Regulation Framework

This chapter presents the framework for the EU Data Protection Regulation Com (2012 11). The different areas of focus help to mitigate the risks which were found during this work.

6.4.1 Scope

This framework serves as a basis for a provider to get an overview of the proposed data protection regulation by the European Commission. It can be used as a guide to consider the most important changes for cloud computing services. The framework highlights what customers but especially providers have to mind and implement to comply with the new regulation. Further, the responsibilities for both the provider and the user are listed within the framework.

6.4.2 Structure

The framework is illustrated at the end of this chapter.

6.4.3 Legal and Organizational Requirements

For a controller to comply with the new EU regulation in the matter of legal and organizational requirements it is important to consider the following points (data protection issues are mainly discussed in the category data protection):

- The Controller needs to designate a representative, which can be any natural or legal person established in the European Union. The representative can be addressed by a supervisory authority instead of the controller.
- Article 22 "Responsibility of the controller" contains the implementation of appropriate measures and strategies as well as the adoption of policies so that the processing of personal data is in compliance with this regulation. The measure shall include:
  - According to Article 28 "Documentation" the controller and processor and, if any, the controller's representative, shall maintain documentation of all processing operations. The documentation should be available, on request, to the supervisory authority.
  - Implementation of data security requirements stated in Article 30 (described in the data protection category)

  - According to Article 33 "Data protection impact assessment", the controller or the processor acting on the controller's behalf has to perform an assessment of the impact of the envisaged processing operations, if the processing operations present specific risks.
  - According to Article 34 (1) and (2) "Prior authorization and prior consultation" the controller or the processor has to obtain an authorization from the supervisory authority prior to the processing of personal data.
  - According to Article 35 (1) the controller and processor shall designate a data protection officer, if the processing is carried out by a public authority; or the processing is carried out by an enterprise with 250 employees or more.

  To ensure the effectiveness of these measures the controller has to implement mechanism for verification. The verification shall be carried out by independent internal or external auditors.

- According to Article 24 "Joint Controller" if a controller decides to determine the purpose, conditions and means of the processing of personal data jointly with others, implies that the joint controllers have to determine for the controller the respective responsibilities for the compliance to the regulation.

- According to Article 26 "Processor", a controller shall choose a processor providing sufficient guarantees to implement appropriate technical and organizational measures as well as procedures in such a way that the processing will comply with the regulation. In particular in respect of the technical security measures and organizational measures governing the processing to be carried out. The processing shall be governed by a contract for the binding of the processor to the controller, in particular the processer shall:

  - act only on instructions from the controller;
  - employ only reliable stuff;
  - implement all required measures according to security of processing;
  - support the controller in complying to the data security obligations of the regulation;
  - hand over all results after the end of the processing;
  - make available all information necessary to control compliance.

The controller and the processor have to document the controller's instructions and the processor's obligations listed. Important to mention is that if a processor processes the data other than instructed by the controller, the processor will be considered as controller according to that processing and has to apply to Article 24 "Joint Controllers". The controller and the processor and, if applicable the representative of the controller,

shall co-operate, on request, with the supervisory authority in the performance of its duties.

6.4.4 Data Protection Requirements

Important to mention for the security of data is again Article 26 which states that a controller has to choose a processor providing sufficient guarantees to implement all technical measures so that the processing will comply with the new regulation. The processing shall be governed by a contract. In other words, the controller has to protect himself legally with a contract; otherwise he will be responsible for data breaches.

6.4.4.1 Data Loss / Data Breach

According to Article 30 "Security of processing", the controller and processor have to ensure with appropriate technical measures an adequate level of security. Both shall take these measures to protect personal data against unlawful or accidental destruction or accidental loss and have to prevent unlawful forms of processing. In particular any unauthorized disclosure, dissemination or access, or alteration of personal data.

- Incident Response / Notification. The Notification of a data breach has to be processed according to Article 31 and Article 32.

  According to Article 31 "Notification of a personal data breach to the supervisory authority", the controller has to notify the personal data breach to the supervisory authority without undue delay and, where feasible within 24 hours after having become aware of it. The processor has to alert and inform the controller immediately after the establishment of a personal data breach.

  According to Article 32 "Communication of a personal data breach to the data subject", the controller has to notify the data subjects after informing the supervisory authority without undue delay.

- Sanctions. A breach could result in a fine up to 1.000.000 EUR or in case of an enterprise up to 2% of its annual worldwide turnover. The fines will be imposed by the supervisory authority.

6.4.4.2 Data / Vendor-Lock in

According to Article 18 "Right to data portability", a data subject has the right to obtain from the controller a copy of data undergoing processing in an electronic and structured format which is commonly used. That means if a controller is choosing a provider the controller is responsible for the provision of those data, which should be stated within a contract.

6.4.4.3 Data Lifecycle

According to Article 17 "Right to be forgotten and to erasure", a data subject has the right to obtain from the controller the erasure of personal data. Further has the controller to implement mechanisms to ensure that the time limits established for the erasure of personal data or for a periodic review of the need for the storage of the data are observed.

6.4.4.4 Data Location / International Transfer

The transfer of personal data to third countries or an international organization is stated within chapter five of the new regulation.

A controller has to consider the following points:

According to Article 40 "General principle for transfers", any processing of personal data to a third country or to an international organization is just permitted if the controller and the processor comply with the conditions of the new regulation.

According to Article 41 "Transfers with an adequacy decision", if the commission states that the third country, territory or the international organization has an adequate level of protection the transfer may take place. Therefore, the commission publishes in the "Official Journal of the European Union" a list of those countries, territories and international organizations with an adequate level of security and a list of those which do not have an adequate level of security.

Article 42 "Transfer by way of appropriate safeguards" discusses the scenario if the commission has taken no decision. In that case, the controller or processor has to adduce appropriate safeguards in a legally binding instrument. These safeguards can be provided by

- Binding corporate rules which shall specify according to Article 43 "Transfer by way of binding corporate rules": their legally binding nature; the structure and contact details of the group of undertakings; the data transfer and the type of processing as well as purpose, the general data protection principles, the acceptance by the controller or processor established on the territory, the mechanisms for verification of compliance with the rules, and more; or
- Standard data protection clauses adopted by the commission and by a supervisory authority; or
- Contractual clauses between the controller or processor and the recipient of the data.

Some exceptions for the transfer of personal data, if the above described points do not exist are stated Article 44 "Derogations".

Figure 6.11 illustrates the framework.

Legal and Organizational Requirements to comply with the General Data Protection			
Responsibilities (Article 22)		**Representative**	**Processor (Article 26):**
Implementation of Appropriate Measures:	- Documentation (Article 28) - Data Security (Article 33) - Data Protection Impact Assessment (Article 33) - Prior Authorization (Article 34) - Data Protection Officer (Article 35) - Documentation (Article 28)	Designation of a Representative in EU	Chosen Processor by Controller shall: - Act Only on Instructions - Employ reliable Staff - implement Required Measures - Support Controller in Complying - Hand over all Results after Processing - Make Available All Information for Compliance
Mechanisms for verification		**Joint controller (Article 24)**	

Data Protection Requirements to comply with the General Data Protection			
Vendor-Lock in	**Data Loss / Data Breach**	**Data Lifecycle**	**Data Location / International Transfer**
Right to Data Portability (Article 18)	Security of Processing (Article 30) Notification to the Supervisory Authority (Article 31) Notification to the Data Subject (Article 32)	Right to be Forgotten and to Erasure (Article 17)	General Principle for Transfers (Article 40) Transfers With an Adequacy Decision (Article 41) Transfer by the Way of Appropriate Safeguards (Article 42)

Figure 6.11: Framework of the EU Data Protection Regulation com 2012 11

CHAPTER 7

Conclusion

Within this work, the terms and basic concepts of cloud computing were defined and the offered services with the focus on legal aspects explained. International and national laws and regulations were explained and the applicable law defined. Further, the upcoming general data protection regulation by the European Commission was discussed. The work captured the critical areas and characteristics of cloud computing. It is concluded that security and privacy are the major challenge customers and providers have to deal with when using or offering cloud computing services. These risks can be generally classified into legal and technical issues. Organizations should be aware of all the risks and concerns which come along. This thesis analyzed the existing work and conditions for an evaluation framework as a guide to secure cloud computing based on the related information and security risks and concerns identified. As areas of requirements for cloud provider were identified: legal and organizational requirements, data protection and technical requirements. With the evaluation framework, we defined there two requirements to highlight the characteristics a cloud provider must posses to be considered as reliable. Further, the work provided a framework which highlights the importance of security measures in accordance to the upcoming EU general data protection regulation. Organizations deciding to use cloud offers in the future will have to deal with many new significant obligations. Also, the providers have to upgrade their policies and security implementations to comply with it. The described framework shows the important points to comply with the obligations of the general data protection regulation. Some companies may see the regulation as a barrier to move into the cloud but the protection of data became an essential part of our society, since data became the new web currency. However, cloud computing will continue growing and the proposal for a major reform of the European Union legal framework on the protection of personal data is an important step towards securing sensitive data in the cloud.

List of Figures

Bibliography

[All10] Cloud Security Alliance. Top threats to cloud computing v1.0. 2010.

[All11] Cloud Security Alliance. Security guidance for critical areas of focus in cloud computing v3.0. 2011.

[All13] Cloud Security Alliance. The notorious nine cloud computing top threats in 2013. 2013.

[AUK12] Manuel Oriol Afnan Ullah Khan. Security risks and their management in cloud computing. 2012.

[BF10] Armando Escalante Borko Furht. *Handbook of Cloud Computing*. Springer Science+Business Media, LLC, 2010.

[Bit06] Bitkom. *Übermittlung personenbezogener Daten.*, volume 2. Recht und Steuer, 2006.

[Bit09] Bitkom. *Cloud Computing - Evolution in der Technik, Revolution im Business*. BITKOM-Presseinfo, 2009.

[Bit10] Bitkom. *Cloud Computing - Was Entscheider wissen müssen*. Leitfaden Cloud Computing, 2010.

[CB11] Jens Nimis Stefan Tai Christian Baun, Marcel Kunze. *Cloud Computing: Web-basierte dynamische IT Services*. Springer-Verlag Berlin Heidelberg, 2nd edition, 2011.

[Cho11] Dimitris N. Chorafas. *Cloud Computing Strategies*. CRC Press Taylor & Francis Group, 2011.

[CM11] Kotze P. Carroll M. Secure cloud computing: Benefits, risks and controls. *Information Security South Africa (ISSA)*, 2011.

[Com12] European Commission. General data protection regulation. 2012.

[ENI09] ENISA. Cloud computing security risk assessment. 2009.

[For09] Jericho Forum. Cloud cube model: Selecting cloud formations for secure collaboration. April 2009.

[Fos02] Ian Foster. *What is the Grid? A three Point Checklist*. 2002.

[Gen04] Alexander Genz. *Datenschutz in Europa und den USA*. Deutscher Universitäts-Verlag/GWV Fachverlage GmbH, Wiesbaden 2004, 2004.

[GH12] ENISA Giles Hogben, Marnix Dekker. Procure secure: A guide to monitoring of security service levels in cloud contracts. 2012.

[Gra10] Wolfgang Graf. *Datenschutz im Überblick*. Facultas AG, 2nd edition, 2010.

[HT10] Joshi Gail-Joon Ahn Hassan Takabi, James. Securecloud: Towards a comprehensive security framework for cloud computing environments. *2010 IEEE 34th Annual*, 2010.

[IF08] Ioan Raicu Shiyong Lu Ian Foster, Yong Zhao. Cloud computing and grid computing 360-degree compared. page 10, 2008.

[KT11] Christian Voigt Kornel Terplan. *Cloud Computing*. Hüthig Jehle Rehm GmbH, 2011.

[LB11] Robert Patt Corner Jeff Voas Lee Badger, Tim Grance. Draft cloud computing synopsis and recommedations. Technical report, National Institute of Standards and Technology, 2011.

[MS11] Georg Meyer-Spasche. *Vertragsgestaltung beim Cloud Computing*. Praxis der Wirtschaftsinformatik, 2011.

[NA10] Lee Gillam Nick Antonopoulos. *Cloud Computing: Principles, Systems, Applications*. Computer Communications and Networks. Springer-Verlag London Limited, 2010.

[Nie09] Paul Nieman. *Bewölkt oder wolkenlos rechtliche Herausforderungen des Cloud Computing*. Kommunikation und Recht, 2009.

[oD11] Australian Government Department of Defence. Cloud computing security considerations. 2011.

[Par08] European Parliament. *Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I)*. Official Journal of the European Parliament, 2008.

[Pol10] Pollirer/Weiss/Knyrim. *DSG - Datenschutzgesetz IdF der DSG-Novelle 2010*. MANZ, 2010.

[RSA09] RSA. Identity & data protection in the cloud. November 2009.

[SHN10] Eui-Nam Huh Sang-Ho Na, Jun-Young Park. Personal cloud computing security framework. *2010 IEEE Asia-Pacific*, 2010.

[Sos11] Barrie Sosinsky. *Cloud Computing Bible*. Wiley Publishing, Inc., 2011.

[TF10] Counsel Katharina A. Weimer Thomas Fischl. Transcending the cloud. 2010.

[WJ11] NIST Wayne Jandsen, Timothy Grance. Guidelines on security and privacy in public cloud computing. *NIST Special Publication 800-144*, 2011.

[XZ10] Hao Li Xuejie Zhang Xuan Zhang, Wuwong N. Information security risk management framework for the cloud computing environments. *2010 IEEE 10th International Conference*, 2010.

[ZC10] J. Zhixiong Chen, Yoon. *IT auditing to assure a secure cloud computing*. 2010 6th World Congress, 2010.