Law and Technology Master Program

TO WHAT EXTENT EUROPEAN END-USERS CLOUD COMPUTING CONTRACTS COULD BE STANDARDIZED TAKING INTO ACCOUNT THE MOST ESTABLISHED CONTRACTS IN USA

MASTER THESIS

AMAIA ONAINDIA PÉREZ

ANR: 936840

SUPERVISOR: KEES STUURMAN

JUNE 2012

Table of contents

LIST OF ABREVIATIONS

Amazon EC2	Amazon's Elastic Compute Cloud
Amazon S3	Amazon Simple Storage Service
ASP	Application Service Provision
AUP	Acceptable Use Policy
AWS	Amazon Web Services
BDSG	Bundesdatenschutzgesetz
CPU	Central Processing Unit
CSA	Cloud Security Alliance
DPD	Data Protection Directive
DRD	Data Retention Directive
eCommerce	Electronic Commerce
ECS	Electronic communication services
EEA	European Economic Area
ePrivacy	Privacy and electronic communication
EU	European Union
FADP	Federal Act on Data Protection (Switzerland)
IaaS	Infrastructure as a Service
ICO	Information Commissioner's Office
IEEE	Institute of Electrical and Electronics Engineers
IP	Intellectual Property
ISAE	International Standard on Assurance Engagements
ISO	International Standards Organization

ISS	Information Society Service
IT	Information Technology
NIST	National Institute of Standards and Technology
PaaS	Platform as a Service
QoS	Quality of Service
SaaS	Software as a Service
SLA	Service Level Agreement
SNS	Social Network Service provider
T&C	Terms and Conditions
ToS	Terms of Service
WP	Working Party
WSLA	Web Service Level Agreement

INTRODUCTION

Research objective

Nowadays, the number of public administrations, companies and individuals willing to contract one of the cloud computing services available through the Internet is growing steadily. However, there are still users who show some distrust towards such kind of services claiming that the risks outweigh the advantages.

Indeed, far from being transparent, some cloud computing contracts do not address clearly certain topics, such as questions concerning data protection and liability issues. Moreover, this lack of clarity may be problematic for both, providers and end-users, and involve legal and commercial risks for them.

Owing to the just mentioned landscape, institutional measures are urged in order to set some stability when contracting such services, and consequently eliminate the complexity revolving around the contracts mentioned above.

The European Commission seems especially involved in cloud computing issues. Thus, on May 2011, the named institution published on its Digital Agenda a consultation whose main goal was to draft a "new strategy" for Europe and exploit the benefits of the clouds[1]. Thus, the Commission was *"inviting all interested parties, in particular cloud developers and cloud users, to explain their experience, needs, expectations and insights into the use and provision of cloud computing.*"[2]

The cited consultation tried to deal with issues such as; standardization of agreements, security and liability matters concerning for instance cross-border transfers, in order to stimulate and trigger a cloud computing environment where citizens and businesses can fairly profit from the technical benefits offered by such development.

From the speech of Neelie Kroes, Vice-President of the European Commission, which took place on 26th of January 2012 we deduce that different actions are being studied with the

[1]Europa press releases Rapid, Reference: IP/11/575 " Digital Agenda: Commission seeks views on how best to exploit cloud computing in Europe" (2011)
<http://europa.eu/rapid/pressReleasesAction.do?reference=IP/11/575&format=HTML&aged=0&language=EN&guiLanguage=en> Accessed 21st January 2012.
The consultation ended in August 2011; however the outcome will take place during 2012.

[2] Ibid.

aim of reaching the cited "new strategy" mentioned above and make Europe "cloud-active"[3]. One of the activities studied is the setting of a European Cloud Partnership, whose first aim will be to "*come up with common requirements for Cloud procurement. For this it will look at standards; it will look at security; it will look at ensuring competition, not lock-in.*"[4] This common approach, which from the speech we presume intends to bring together public authorities and cloud providers, could also be applicable to enterprises and users standards since "*there is no reason why procurement by private businesses and organizations would not adapt in this direction as well"*[5].

From this speech we can deduce that one way to reach this so desired common approach to a more cloud friendly environment would be by setting a standard model when contracting cloud computing services. Like this, all different cloud computing contracts could be harmonized.

This opinion was already pointed out by many European businesses, which in a hearing that took place in November 2011 claimed that "*Cloud service providers should be required to adhere to EU standards for the protection of personal and company data (laid down, for example, in EU Standard Contractual Clauses)"*[6]. Therefore some end-users of cloud services urge the setting of certain standards. More concretely, from the hearing just cited, we see that standards referring to data protection have already been claimed necessary, which, in my opinion, could fit in a more general cloud computing contract standard framework.

Owing to the situation explained above, my research question is the following:

To what extent European end-users cloud computing contracts could be standardized taking into account the most established contracts in USA.

Thus, the main objective of my thesis will consist of analyzing how European end-users Cloud Computing contracts should best be approached. Could the most favorable US' provisions be suitable in the European contract structure?

---

[3] Kroes N. Reference: SPEECH/12/38 "Setting up the European Cloud Partnership World Economic Forum Davos, Switzerland, 26th January 2012" (2012), Europa press release . <http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/12/38&format=HTML&aged=0&language=EN&guiLanguage=en> Accessed 27th January 2012.

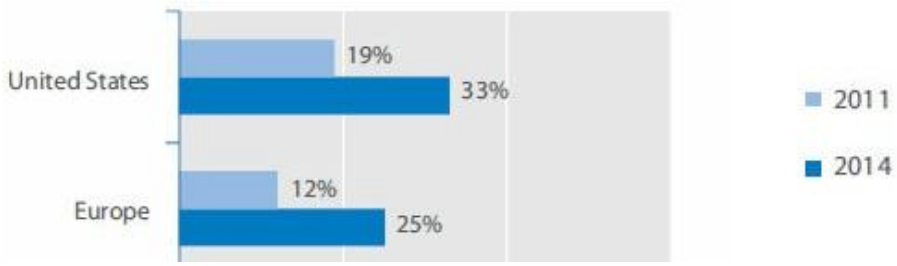
[4] Ibid.

[5] Ibid.

[6] Commission of the European Communities, Information Society & Media Directorate-General, Software & Service Architectures, Infrastructures and Engineering Unit. "Cloud Computing Hearing with Users: Meeting Note" (2011). Europe's information society, Thematic portal., 4.
< http://ec.europa.eu/information_society/activities/cloudcomputing/docs/hearingreport-usersv2.pdf> accessed 27th of January 2012.

We chose the USA as comparative scenario to Europe, due to the importance and influence which nord-american companies have had in developing the services nowadays known as cloud computing. Actually, *"many of the companies that have been driving and leading the cloud computing phenomenon are US-based, such as Amazon Web Services, Google, IBM, RackSpace, Microsoft, Apple, and Oracle"*[7]. Additionally, it is worth to say that cloud computing services have been accepted and developed at a higher speed in USA. For instance, while in 2011 the 19% of the US companies had adopted any of the cloud computing services, the percentage presented in Europe was a 7% lower, reaching the 12%.

Graphic showing the percentage of companies in USA and Europe having adopted cloud computing services in 2011, and their expected percentage for 2014.[8]



That is why we will analyze which US-based providers' clauses could actually fit into the European cloud computing scenario and boost it to reach the already mentioned "cloud active environment" proposed at the European Commission.

Research method

We divided the Master Thesis into four chapters in order to answer the research question.

In the first chapter, we will introduce the basic scenario of cloud computing. We will start explaining what cloud computing is. Thereafter, we will address the most relevant features determining the relationship between end-users and cloud-providers, for further finishing displaying a general overview about the main advantages and drawbacks presented by cloud computing contracts. The cited explanation will be based on literature.

---

[7] McKendrick J. "US Lags Much of World in Cloud Computing Adoption: Study" Forbes (2012). <http://www.forbes.com/sites/joemckendrick/2012/03/29/us-lags-much-of-world-in-cloud-computing-adoption-study/>. Accessed 17th May 2012.

[8] Ibid.

In the second chapter, we will illustrate the overall structure of cloud computing end-user contracts in both the USA and the European landscape. We will base my comparison on an existing study conducted by the Queen Mary University[9]. High level comments will be given at the most relevant provisions to underline the main differences we might come up with over the evaluation. A brief background description will be presented when relevant to understand the main differences seen.

This general landscape study will be based on three US-based and three European-based providers contracts (Terms and Conditions and Privacy policies available on the providers' website) offered by different companies. While USA contracts refer to the most representative companies providing cloud services, the European are selected amongst the current most progressive cloud computing providers[10].

All these contracts, composing the base of this Master Thesis, were selected taking into account the variety of services offered by cloud providers. Consequently, in order to make the comparison more realistic, we chose two contracts (from the US and European based provider respectively) for each kind of service available (SaaS, IaaS and PaaS). Note that all the European contracts are from cloud providers based in different countries.

	US PROVIDER	**EUROPEAN PROVIDER**
SAAS	Salesforce[11]	Twinfield[12] (based in The Netherlands)

[9] Bradshaw S., Millard C. and Walden I. "Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services" (2010) Queen Mary University of London, School of Law. Legal Studies Research Paper No.63/2010 <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1662374> Accessed 25th February 2012.

[10] Cloud Tweaks plugging into the cloud "Top 25 European Cloud Computing Rising Stars To Watch – Complete List." (2011) <http://www.cloudtweaks.com/2011/04/top-25-european-cloud-computing-rising-stars-to-watch-complete-list/>. Accessed 22nd February 2012.

[11] Salesforce.com "Salesforce Master Subscription Agreement" (2011) <http://www.salesforce.com/assets/pdf/misc/salesforce_MSA.pdf> Accessed 20th February 2012. Attached as ANNEX 1.

[12] Twinfield.nl "General Terms and Conditions of Twinfield for subscribers" (2012) <http://www.twinfield.nl/wp-content/uploads/2012/01/AV_Twinfield_2011-SUBSCRIBERS_ENGLISH_v1.pdf> Accessed 20th February 2012. Attached as ANNEX 2.

IAAS	Amazon S3[13]	Cloudee[14] (based in England)
PAAS	Microsoft Azure[15]	CloudControl[16] (based in Germany)

Additionally, we chose one contract provided by a Swiss cloud provider called "CloudSigma"[17].Such contract will not be analyzed in depth since Switzerland does not form a part of the European Union, however, short comments will be pointed out where relevant.

In the third chapter, we will briefly explain the legal basis which will constitute the ground for the proposed contract. Such explanation will be focused from both a provider and an end-user perspective. This chapter will be supported by current legislation, literature, official documents and hearings.

The fourth chapter will reveal a standard contract, which European cloud providers offering services to end-users should adhere to. This contract will try to balance the interest of both cloud providers and end-users and take into account the possible advantages and drawbacks that standard contracts could imply.

We will dedicate the final chapter to conclusions and recommendations set based on them.

[13] Amazon.com "Amazon Web Services Customer Agreement" (2012) <http://aws.amazon.com/agreement/> Accessed 20th February 2012.
By the time of writing the theses, Amazon updated a new version of the agreement; however none of the changes affect the clauses analyzed over the thesis.
Attached as ANNEX 3

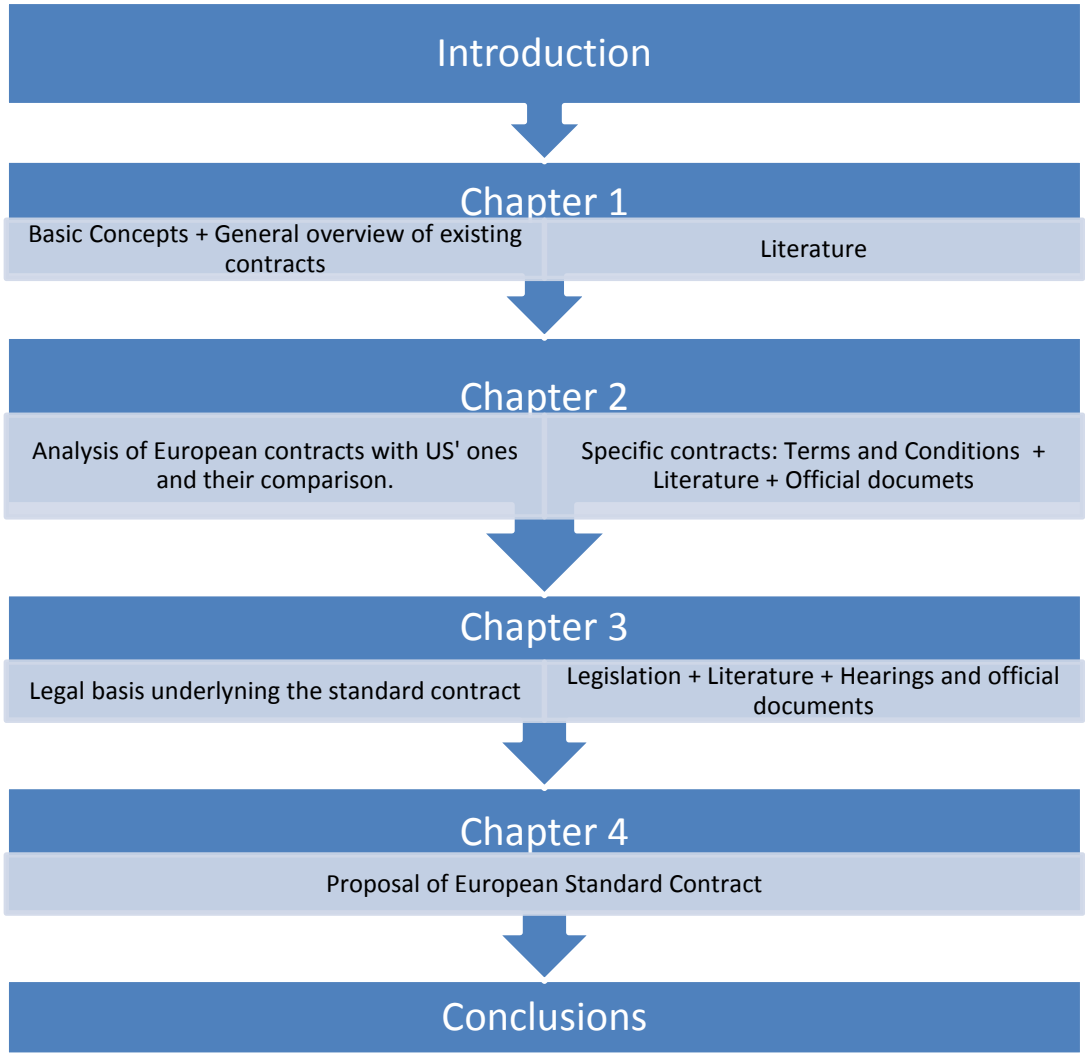
[14] Cloudee.eu "Cloudee Terms and Conditions" (2011) <http://www.cloudee.eu/terms> accessed 20th February 2012.
Attached as ANNEX 4

[15] Windowsazure.com " Microsoft Online Subscription Agreement" (2012) <http://www.windowsazure.com/mosa.aspx?country=us&locale=en-us> accessed 20th February 2012.
Attached as ANNEX 5

[16] CloudControl.com "CloudControl Terms and Conditions" (2011) <https://s3-eu-west-1.amazonaws.com/cctrl-www-assets/20110519_Terms_cloudControl.pdf> accessed 20th February 2012.
Attached as ANNEX 6.
By the time of writing the Thesis, the website was updated, and therefore the clauses cited in the paper might not correspond with those of the latest updated version of 29th March, 2012 <https://www.cloudcontrol.com/tos>.

[17] CloudSigma.com "Terms of Service" (2011) <http://www.cloudsigma.com/en/platform-details/legal?t=0> accessed 20th February 2012.
Attached as ANNEX 7.

Thesis Structure



CHAPTER ONE: Cloud computing services: Basic concepts.

1.1: What is cloud computing?

In order to understand what cloud computing services are, it is essential to explain other concepts first. Indeed, cloud computing is the result of a steady evolution[18] of IT services which started with what is known as IT outsourcing.

In IT outsourcing, a customer enters into a contract with a supplier regarding the performance of IT services on behalf of the former.

The next step came with the ASP "Application service provision". The main difference with respect to the modality explained above is that the software used by the supplier, in this second scenario, is not in on-site servers but in an off-site location.

Finally, we reach the step of cloud computing. Under a cloud agreement, different resources are provided as a service. In the following sub-section the different categories of cloud computing are explained.

Even though there is no unique definition about what cloud computing services are, the most extended is the one given by the National Institute of Standards and Technology (NIST) which in January 2011 defined cloud computing as follows "*Cloud computing is a model for enabling ubiquitous, 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."*[19]

However, we personally favor the following definition as being the most complete, gathering all the characteristics of cloud services: *"It is an information technology service model where computing services (both hardware and software) are delivered on-demand to customers over a network in a self-service fashion, independent of device and location. The resources required to provide the requisite quality-of-service levels are shared, dynamically*

[18]Joint A. and Baker E. "Knowing the past to understand the present- issues in the contracting for cloud based services"(2011), computer law & security review 27 , 408 .
<http://pdn.sciencedirect.com/science?_ob=MiamiImageURL&_cid=271884&_user=522558&_pii=S0267364911000689&_check=y&_origin=article&_zone=toolbar&_coverDate=31-Aug-2011&view=c&originContentFamily=serial&wchp=dGLbVlB-zSkWz&md5=4b223978c2cde7549052c0325fc5122c/1-s2.0-S0267364911000689-main.pdf> accessed 1st February 2012.

[19] Mell P. and Grance T. "The NIST Definition of Cloud Computing" (2011). NIST National Institute of Standards and Technology,2.
<http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf>, accessed 1st February 2012.

scalable, rapidly provisioned, virtualized and released with minimal service provider interaction. Users pay for the service as an operating expense without incurring any significant initial capital expenditure, with the cloud services employing a metering system that divides the computing resource in appropriate blocks."[20]

To summarize this, the new feature offered by cloud computing is that the applications or software (computation or storage services) we pay for, are executed or maintained somewhere in the cloud. Therefore end- users do not need to operate such instruments in their own infrastructure.

1.2: Cloud Computing Systems

When we talk about cloud computing, we need to be aware of the diversity of contracts existing behind it and all the points which need to be taken into consideration before entering into the contract.

While weighing whether to contract a cloud service or not, it is essential to clearly understand the architecture of the cloud service. Moreover, end-users willing to enter into the cloud contract should make an evaluation of their specific situation and features in order to arrange it with the most suitable cloud provider.

In the next sections, we will discuss the different delivery models, deployment models, quality of service and security issues, as the main points of interest regarding contracts for cloud services.

1.2.1 Delivery models

Delivery models refer to the different kind of services available under cloud computing services which can be delivered by cloud-providers. The end-users need to select the delivery model which best fits their features and objectives.

As cloud computing is a trend in constant evolution, many different services are likely to evolve over the years. We will focus on the services already classified by the NIST[21], which

[20] Marston S.., Li Z., Bandyopadhyay S. and Zhang J. "Cloud Computing – The Business Perspective" (2009) University of Florida.-Warrington College of Business Administration, 3. <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1413545> accessed 1st February 2012.

[21] See Supra n19, 2.

are Software as a Service, Infrastructure as a Service and Platform as a Service to keep explanation clear.

Additionally, we would like to point out that in some occasions end-users may be involved in more than one service without even being aware of that situation. A cloud provider can purchase another service from another cloud provider, being therefore the customer of the first supplier involved in both services[22]. This is known as a "chain" of services.

A. Software as a service (SaaS).

The first category refers to the situation where Software is offered as a service ("SaaS"). Here, the software is run by the supplier at its server, and end-users can just have access to it over the Internet. Such software is usually designed to support multiple customers at the same time. Through SaaS, users do not need to license or buy the software, since they do not need to install it in their own computers and update it. It is the supplier who is in charge of the update, deployment, maintenance and security of the service. Hence, he is the one who has the highest control over the contracted service. Normally the fee to pay is calculated depending on the number of the software users.[23]

End-users of this model are businesses and individuals since both can indistinctly benefit from the reduced costs of configuration, maintenance and support required by such service.

Some examples of SaaS are Salesforce.com[24] and Twinfield[25].

B. Infrastructure as a service (IaaS).

Through this service, an end-user can make use of hardware remotely accessing to a virtual server as if it were in his location. Thanks to this service, end-users can run any application or software in the virtual server and do not need to spend money in acquiring their own data centers[26]. In this second scenario end-users pay "as they go". This means that their service payment will be calculated in function of the resources they use (for example storage space needed, CPU per hour, etc.), which can be easily adapted to their needs.

---

[22] Da Correggio Luciano L. and Walden I. " Ensuring competition in the Clouds: The role of competition Law?" (2011) Social Science Research Network,2. <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1840547> Accessed 26th of March 2012.

[23] See Supra n18, 408.

[24] For more information check < http://www.salesforce.com/au/saas/what-is-saas/> accessed 21st February 2012.

[25] Twinfield T&C clause 12.3 (See Supra n12).

[26] See Supra n18, 409.

This is the case of Amazon's Elastic Compute Cloud (EC2), which uses a "virtual server". End-users utilize part of the data center, instead of some hardware as such. In this case, the provider is responsible for the performance of the server and its basic hardware. Meanwhile, end-users are responsible for the operating system running and all the applications of the server[27]. From the terms of service of the EC2 offered by Amazon, we can read "*You are responsible for maintaining licenses and adhering to the license terms of any software you run."*[28]

Nevertheless, simpler hardware can be contracted. That is the case of Amazon S3, which refers to plain storage capacity.[29]

The subscribers of this model are both businesses and individuals.

C. *Platform as a service (PaaS).*

This kind of service is similar to IaaS because end-users have access to a virtual server which, in this third scenario, has already been pre-configured by the provider who runs the operating system[30]. The responsibility to maintain server and hardware relies on the latter, while end-users only have to manage the software running on it[31].

The main subscribers of PaaS are usually businesses such as vendors of Software or IT services providers, and even individuals willing to develop SaaS.

Clear examples of PaaS are Microsoft's Windows Azure[32] and CloudControl[33].

1.2.2 Deployment models[34]

[27] See Supra n18, 409.

[28] AWS Service Terms (2012), clause 4.1 <http://aws.amazon.com/serviceterms/> . Accessed 21st February 2012.

[29] For more information check <http://aws.amazon.com/s3/#functionality> accessed 21st February 2012.

[30] See Supran18, 409.

[31] Ibid.

[32] Microsoft Online Subscription Agreement Clause 2.d (See Supra n15).

[33] CloudControl T&C, clauses 4.1 and 5.3 (See Supra n16).

[34] The NIST identified them. See Supra n19, 3.

There are four types of deployment cloud models, all of them with different characteristics. End-users need to study their own situation in order to choose the deployment model that best fulfills their requirements.

A. Public

A public cloud involves the idea of sharing the cloud infrastructure offered by a sole provider, among a multitude of users; such as the public in general or enterprises.

This kind of cloud is ideal for small or medium sized businesses.

B. Private

All the cloud services are delivered to a single end-user. While the advantages of public clouds are kept, a private one offers more control over the infrastructure since the end-user can manage it. The enterprises willing to contract through this kind of cloud are normally larger organizations.

C. Community

A community cloud is shared by different organizations which share among them the same interests and features. Such cloud can be operated by one or more of the organizations composing the community, or it can be managed by a third-party.

D. Hybrid

This last infrastructure is the result of the mixture of two or more of the deployment models explained above. Each cloud remains unique but controlled by technology which enables the portability of either the data or applications run. The most common trend is to keep both businesses and personal data in the private cloud, while the non-relevant information is outsourced to the public cloud

1.2.3 Quality of service (QoS):

Through QoS, cloud-providers give some guarantees to their users about the service they will provide, and consequently, assume to deliver predictable results up to a level. One way to set those facility levels is through Service Level Agreements (SLAs).

SLAs are contracts signed between the cloud provider and the end-user, where the conditions and the level of the service to be delivered are agreed upon.[35] This kind of

[35] Examples of current SLAs are the following ones:
Amazon S3 <http://aws.amazon.com/s3-sla/> accessed 21st February 2012.
Windows Azure <http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=24434> accessed 21st February 2012.
CloudSigma "<http://www.cloudsigma.com/en/platform-details/legal?t=3> accessed 20th February 2012.

agreements, not always available when entering into a cloud computing contract, commonly guarantee a 99% of service accessibility and display a mechanism to compensate end-users when such level is not reached. Usually, SLAs include a list of exclusions since SLAs are not applicable to all situations.[36]

Not surprisingly, SLAs do not cover all the end-user's enquiries, therefore a balance between the end-users' and the providers' claims needs to be found when committing to an agreement.

In a cloud computing context, it would be better to talk about Web SLA(WSLA), commonly used to monitor the services deployed by the cloud provider. Although different parties might be involved in this SLA (cloud provider, service's end-users, and third parties[37]), the contract is binding only for the signatory parties which are the provider and the end-user.

Therefore, a standard SLA should be composed of three components: parties involved, service definitions and contractual parties' obligations. The main problem which may arise from this context is how to agree upon the setting of best practices in a cloud computing scenario; such as measurement services, evaluation services and management services.[38]

1.2.4 Security

Businesses seem concerned about the fact that their data will be managed by entities different to themselves. This fact was reflected in a survey carried out by the Cloud Computing Alliance and IEEE published the first of March 2010. *"It's clear from the survey's findings that enterprises across sectors are eager to adopt cloud computing - but that security standards are needed both to accelerate cloud adoption on a wide scale and to respond to regulatory drivers".*[39]

---

[36] Commonly Cloud-providers will not be liable for the performance and accessibility of the service when it is not available for causes outside their control, for instance, a failure of internet connection. Therefore, as Twinfield expresses in its clause 18.2 T&C, "*accessibility is not understood to the existence of a working point-to-point connection between the systems of Subscriber and the Servers*".

[37] These third parties refer to companies which are in charge of either the analysis of security measures carried by cloud providers or take actions when there is any violation.

[38] See Patel P., Ranabahu A.and Sheth A. "Service Level Agreement in Cloud Computing" (2009), Knoesis Center, Wright State University, USA and DA-IICT, Gandhinagar, INDIA,7.
<http://knoesis.wright.edu/library/download/OOPSLA_cloud_wsla_v3.pdf> accessed 20th February 2012.

[39] Reavis J., **"**Survey by IEEE and Cloud Security Alliance details importance and urgency of Cloud Computing Security Standards" (2010) IEEE Standards Association. <http://standards.ieee.org/news/2010/cloudcomp.html> accessed 21st february 2012.
At this same link, the main findings of the survey are available.

Moreover, each of the deployment models just explained present different levels of security, which will be introduced briefly.

With regards to SaaS, the fears held by end-users revolve around the way cloud providers store their data. This fact is probably due to the lack of information about how the data is secured and what would be the consequences in case of data loss by cloud providers. We cannot forget that the providers are in charge of delivering on all the security measures. It is difficult for the user to know when such measures are effectively in place and whether they are protective enough.[40]

IaaS services offer a basic security level only. While the provider is only responsible for the setting of basic security measures regarding the maintenance and running of the server and its hardware, end-users need to take care of the operating system and all software of applications running in the server, including the security controls.[41] This is the case of Amazon, which in its security policy says: *"You are responsible for properly configuring and using the Service Offerings and taking your own steps to maintain appropriate security, protection and backup of Your Content".*[42]

Developers of PaaS do not really know what happens behind the application they build up. Despite the control given to end-users when creating their application, the security issues behind the application, such as host or intrusion to the network by hackers, remains in the provider's hands being responsible for the provision and maintenance of the operating system and its hardware.[43] Therefore, like at the SaaS, doubts are still raising when evaluating the efficiency of the measures taken by the provider, since users cannot easily estimate whether they are correctly working or not.

From there we see that IaaS providers exclude the obligation of taking security measures for safeguarding end-user content from their duties.[44]. In fact, it is an end-user obligation to set the height of the security level they might need to protect their content or application. Meanwhile, SaaS and PaaS providers are obliged to take some secure measures (set by default) in order to safeguard end-user content. However, such measures are not always

[40] S. Subashini and V. Kavitha "A survey on security issues in service delivery models of cloud computing" (2010) Journal of Network and Computer Applications, 3-4.
<http://dblab.mgt.ncu.edu.tw/%E6%95%99%E6%9D%90/991-seminar/10.pdf > accessed 21st February 2012.

[41] See Supra n18, 409.

[42] Amazon Web Services Customer Agreement, clause 4.2. (See Supra n13).

[43] See Supra n18, 409.

[44] Note that here "content" refers to any kind of data not categorizes as "personal data". As we will see later on, "personal data" needs to be regulated by specify Directives which try to harmonize within the EU Member States a minimum level of security measures, when processing and securing it.

available for end-users, who need to rely on and trust their providers when processing and keeping their content.

From there we deduce that the general level of security, from an end-user perspective varies among the different delivery models available in the market, being the most secure ones SaaSs followed by PaaSs and IaaSs respectively.

1.3: Advantages and Drawbacks

The advantages and drawbacks present in cloud computing services can differ from one provider to another; however, to make it simple, the explanation below refers to general characteristics.

There are five main features which make cloud computing an attractive option for end-users.

The first one refers to cost savings. Not having to invest in infrastructure, users save money on hardware, software, licenses and other additional services.[45] Actually, the fact that cloud services are accessible remotely removes the cost of storage and configurations what really makes cloud computing so profitable from an end-user perspective. Such low barriers of entrance[46] make cloud computing services very attractive.

This idea is tightly connected to the multi-tenancy model presented by cloud services which allow achieving economies of scale. In this way, majority of the cost can be shared among all the users of the service. That is the case of maintenance and support costs.[47]

Moreover, end-users become independent with regard to location[48], since they have access to the services contracted from everywhere. This point is extremely important for businesses because otherwise their staff could not have an access to the content they might need in an out of office environment.

Additionally it allows the access to the most updated technology.[49] Since the provider is the one who controls software or hardware, the end-user can take advantage of the latest

[45] Buono L. "The Global Challenge of Cloud Computing and EU Law", (2010), The European Criminal Law Association's Forum,117. <http://www.mpicc.de/eucrim/archiv/eucrim_10-03.pdf>. Accessed 24th of March 2012.

[46] Ibid.

[47] Ibid.

[48] Ibid.

[49] Ibid.

technology and its updates, most of the times not paying extra money for that, since the former provides all end-users simultaneously.

Finally, cloud services also offer immediate access to a broad range of applications[50], which is translated into extreme flexibility for end-users. Hence, cloud providers can very quickly broaden or narrow down their user capacity of the service paying only for what they use.

Nevertheless, despite the several advantages offered by cloud computing services, there are also some drawbacks which should be object of our attention. Hence, the next section will list the main drawbacks of cloud computing services.

The first and major concern relies on a topic already pointed out, which is the security and privacy issue. It is important to consider that cloud service end-users are handing their data to providers operating and delivering their services over the internet, thus being susceptible to viral and other attacks. Different instruments to protect the end-user content are available, such as accounts protected by passwords and encryption techniques. However, these measures are not always provided by all cloud providers, and even if they are, end-users do not always have the means to determine if they are working effectively. Moreover, certain kind of content (such as personal data) requires higher security requirements, which in many case, are not properly displayed and explained to end-users.

A second aspect to take into account is the dependency that end-users might have on their cloud providers, who are the ones to maintain, update and manage the software. This situation is reflected in the lack of information which end-users know about provider policies in certain issues such as disaster recovery or return of information. Additionally, end-users may want to change their data or application from one provider to another (data portability), or simply extract them from the cloud (reversibility), something that is not always an easy task since users might be "locked-in" to their supplier in case they have not agreed upon an exit plan.[51]

To sum up, we would like to say that before entering into a cloud computing agreement, end-users should carefully weigh both favorable and adverse points of cloud services. A way to do that is through prudently examining all the information displayed in the provider contract details, which unfortunately do not always address to end-user concerns in a sufficient way. End-users need to be aware of the risks that cloud services may involve for the security and privacy of their data.

---

[50] Ibid.

[51] Vincent M. and Hart N., "Legal issues in the Cloud - Part 4" (2011) CIO. <http://www.cio.com.au/article/382657/legal_issues_cloud_-_part_4/>. Accessed the 26th of March 2012.

Apart from the explanation above, there are some legal issues which add some difficulty to the cloud landscape. These legal aspects will be briefly discussed when analyzing the contracts in the next chapter.

CHAPTER TWO: General overview of USA and Europe cloud computing landscape. Comparison of contracts.

In order to start drawing the general overview of cloud services, it is necessary to say that the current scenario of cloud contracts is composed by two different types of documents. The first one refers to an "add-on" contract, which is standard for all end-users, while the second one implies the negotiation of all the clauses with a specific end-user. In this chapter just terms and conditions available on the internet will be analyzed. .

Terms and Conditions (T&C) refer to several documents governing the relationship between cloud-providers and end-users. The most common documents composing them are four (terms of use, SLA, acceptable use policy and privacy policy), despite the fact that not all of them are available or provided by the cloud- provider chosen.

In this chapter we will focus on the analysis of the most important provisions from an end-user perspective (both businesses and consumers[52]), being: data protection, intellectual property rights, confidentiality and disclosure, warranties and disclaimers, limitations of liability, indemnifications, law and jurisdiction, termination and finally monitoring by provider.[53]

In order to proceed to the analysis of the contract provisions, we took as a base the study conducted by the Queen Mary University of comparison of Cloud Contracts[54].

2.1 Data Protection

The scenario presented in both areas of study is quite different. This is fundamentally due to the legislation applicable to this matter.

Europe has a supra-national legislation implemented into the law of all Member States in which the principles for the treatment of personal data are specified. On the other hand, the USA only regulates this issue regarding the collection of data by federal government.[55]

[52] Special attention will be paid to consumer protection laws when relevant.

[53] The clauses chosen are those which may have a greater impact on the end-users interests. While some of the provisions do not show a huge variation from one provider to another, others do. Besides, theses contrasts may even seem more sharped between the two scenarios chosen (EU-based provider and European-based provider). As explained in the introduction, the aim of this chapter is to detect which is the trend followed by US-providers and see whether such tendency would fit in a standard cloud computer contract within the European framework.

[54] See Supra n9, 16-40.

2.1.1. USA:

The USA has no complete data protection legislation and therefore its approach to this issue is very limited. The only available laws making reference to this topic are focused on public sector transfers (they regulate the transfer of personal data among the governmental entities), and on some industries.[56]

Due to this situation, no special treatment is given to end-user "personal data", which is treated at the same level as the rest of their data not likely to identify any person.

A. Security measures:

The lack of a standardized legislation makes it possible for cloud providers to set different levels of security measures, all of them being legitimate. Thus, we see the following examples.

Amazon states in this respect that end-users must take: *"own steps to maintain appropriate security, protection and backup of Your Content, which may include the use of encryption technology to protect Your Content*"[57]. Reasonable measures are provided to secure end-user content; who are responsible to back up their content. Thus, Amazon S3, offers the possibility to encrypt end-user content through four different modalities.[58] However, it is their responsibility to make sure that his content is properly protected. Indeed, on the disclaimer we found no kind of warranty for security, loss or damage of content.

As we already saw in the first chapter, IaaS' end-users are required to take care of the security controls they are willing to set. However, the surprising fact comes when we see that such clause is applicable to all the services offered by Amazon[59]. Therefore, Amazon seems to deny the European reality for data processors, which, within the EU, is mandatory. [60]

---

[55] Stratford J.S. & Stratford J. "Data Protection and Privacy in the United States and Europe", (1998) Yale University, 17-18. <http://www.iassistdata.org/downloads/iqvol223stratford.pdf>. Website accessed the 23rd February 2012.

[56] Ibid.

[57] AWS Customer Agreement, clause 4.2 (See Supra n13).

[58] Amazon Simple Storage Service (Amazon S3) < http://aws.amazon.com/s3>. Accessed 25th February 2012.

[59] No matters if it is an IaaS, SaaS or PaaS service.

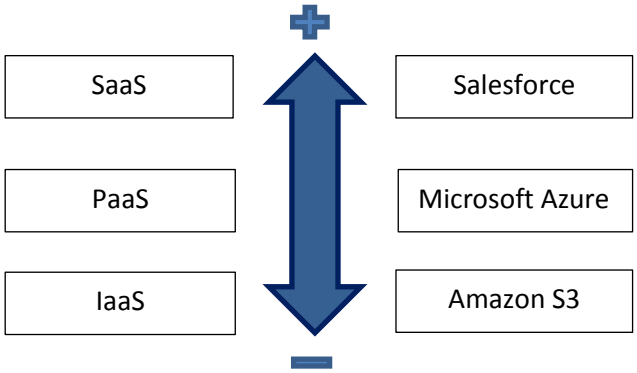
[60] The DPD in its article 4 expresses in which circumstances non-European controllers might be subjected to the Directive.

The article 4.1 (a) of the DPD claims its applicability when *" the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies*

An intermediate position is presented by Microsoft Azure, which in its privacy policy, after explaining the technical and security measures taken to protect the end-user information from unauthorized access, use or disclosure (services are just accessible through password and when the information is transmitted, it is encrypted first), expressly says that end-user have the responsibility to determine whether the security level offered by the company meets their personal requirements. Therefore we deduce that the preservation on the data integrity relies on the end-user who is responsible for meeting its own security requirements.[61]

Similarly Salesforce maintains the use of appropriate administrative, physical, and technical safeguards for the protection of security, confidentiality and integrity of end-user data. It is in its privacy policy where it details the utilization of server authentication and data encryption for guarantying the accuracy of the data. Furthermore, the company offers the possibility to its end-users to configure the security settings they might want.[62]

At this point we find out that the security measures set by the different providers reflect the different level of security offered by the nature of the cloud-service as such.



with the obligations laid down by the national law applicable". Although Amazon has a data center in Ireland, this cannot be defined as establishment. See Hon K., Hörnle J. and Millard C. " Data Protection Jurisdiction and Cloud Computing – When are Cloud Users and Providers Subject to EU Data Protection Law? The Cloud of Unknowing, Part 3"(2011) Queen Mary University of London, School of Law Legal Studies Research Paper No 84/2011,21.
< http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1924240>. Accessed 7th June 2012.

Therefore we are obliged to apply the article 4.1 (c) DPD which says that controllers may be subjected to this Directive, even if they are " not established on Community territory", when they make use equipment within a Member State, for the processing of the data. What should be understood as "use of equipment" rises some doubts. From the WP 56 page 9 we see that servers could be described as equipment, apart from other software devices such as cookies.

This means that if Amazon processes "personal data" (being the controller of such data as well) using its Irish server or cookies in a computer located within a Member State, it would be infringing the security measures obligation stated for controllers and processors displayed under the article 17 DPD.

[61]See "Microsoft Online services Privacy Statement" (2010) <http://www.microsoft.com/online/legal/en-us/mos_privacy_statement_full.htm>. Accessed 23rd April 2012.

[62] Salesforce Master Subscription Agreement clause 4.2 (see Supra n11) and "Salesforce Privacy Statement" (2010) clause 11 <http://www.salesforce.com/company/privacy/full_privacy.jsp> Accessed 23rd April 2012.

Almost all the providers have in place "reasonable measures" for protecting end-user data. However, they are those ones who need to take extra security measures for safeguarding the content they might deem requires higher protection.

We personally think that end-users do not have any kind of security when cloud providers process their content. This situation seems especially worrying when we talk about "personal data", because each provider can put in place different security measures not safeguarding the data properly against unlawful access, transfers, etc. As we have seen, the DPD may be applicable even to non-European providers, nevertheless they do not all comply with its wording (art 17). However there is no effective way to enforce its applicability by non-European providers. If the end-user does not realize the low security measures set by the provider, he could be affected negatively, because his personal data would not be protected enough against intrusions, unlawful processing etc.

B. *Location and transfer of data.*

The same problem arises when talking about data transfers and location, because there is no rule regulating the cases under which the transfer to third counties should be restricted.

In the clause 7 of Salesforce privacy statement, we see how the company claims that they may transfer and access data about their customers around the world. Microsoft deals with this issue in a similar way, saying that the information collected can be processed or stored in any country where the company, its affiliates, or its subsidiaries or service providers maintain facilities[63].

Therefore, in both cases, end-users may not know where their data is processed or transferred to, as these providers are not obliged to notify these operations to them. In my opinion, these unequal relationships result in a lack of end-user knowledge about how their data is treated, because the security measures set in place by cloud providers around the world may vary drastically.

The most secure position is the one held by Amazon, which is the only provider that in its customer agreement offers end-users the possibility to choose the region where they want their data to be stored, transferred and processed. The different regions available are explained in the Amazon S3 overview[64]. This option seems more favorable to end-users who can choose the region, which fits their need in advance. From the same document we read that choosing a close region may increase the speed of access to the infrastructure and improve the general performance of the service contracted.

[63] See Supra n61.

[64] See Supra n58.

Additionally, it is worth to point out that the three analyzed contracts refer to their participation in the European Safe Harbor program. Otherwise European personal data could not be transferred to a US company for not complying with "an adequate level of protection"[65].

Table 1.

USA summary.
• **Security measures and location/transfer rules:**
There is a lack of regulation, therefore the protection of personal data should be granted by end users' demands (negotiation one to one).
Contracts in practice: Both, security measures and location/transfer rules are different among cloud provider companies.
Nevertheless,we found very interesting the option available at the Amazon contract where end-users are those who can choose the region where their data is going to be transfered and processed. (It could be applicable to Europe).

2.1.1 Europe

The Data Protection Directive is applicable to the processing of personal data by automatic means. The WP, defined "personal data" as *"any information relating to an identified or identifiable natural person*"[66]. From there we could deduce that the DPD would only apply to natural persons, however, this Directive also covers "*information relating to businesses or to legal persons"*[67] when such information identifies its personal owner[68]. Therefore the DPD requirements might also be applicable to legal persons' information. This clarification is vital, because we need to remember that businesses are also cloud computing services' end-users.

Hence, when cloud providers process or store "personal data", they need to apply the just cited Directive.

[65] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of Individuals with regard to the processing of personal data on the free movement of such data, *OJ L 281 , 23/11/1995, article 25.1.* <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML>, accessed on the 23rd of February 2012. Hereinafter the " Data Protection Directive" (DPD).

[66] Opinion 4/2007 on the concept of personal data , 01248/07/EN WP 136 (2007),6. <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf>. Accessed 4th June 2012.

[67] Ibid, 23-24.

[68] Ibid.

When applied to cloud computing, there are three main obstacles to take into account. These pitfalls have already been pointed out by Paolo Balboni, Executive Director of the European Privacy Association[69];

- Definitions of data controller and data processor; these definitions are not clear, what makes the allocation of duties and liabilities difficult. Moreover such distinction is also important to know the application of DPD to non-European providers[70].
- Security measures[71]: There is a lack of harmonization among countries, which means that there are different data security levels. Consequently different countries offer different levels of protection from an end-user perspective, while from a cloud provider perspective it is difficult to comply with all security measures through the countries.
- Geographical location of data and transfer.[72] Concerns rise about the jurisdiction to be applied to the data.

A. *Data controller and Data Processor*:

The DPD clearly defines both concepts in its article 2. Nevertheless the distinction may seem quite confusing in the cloud computing scenario.[73] The determination of both concepts is vital, since stricter obligations are attributable to the controller[74] over the DPD articles 6, 7, 12, 10 and 17.1 .

The Article 29 Working Party (WP) 169 tried to clarify both terms, but the distinction is still not clear.[75]

[69] Balboni P. "Data Protection and cloud computing: the need for global standards" (2011) Youtube <http://www.youtube.com/watch?v=b7u-L9yho44>, video accessed the 22nd February 2012.

[70] The scope of cloud providers obliged by this Directive is to be found in the article 4 DPD. However such applicability was already explained above.

[71] DPD Article 16 and 17 (See Supra n65).

[72] Chapter IV of the DPD displays that the transfer of personal data only can take place if the third country (outside the EEA) in question ensures an adequate level of protection for the individual. End-users, as data controllers, might be responsible for guarantee an adequate level of protection on its data (or its staff, etc). Therefore it is essential for them to know where the cloud-provider will process and transfer the data to.

[73] DPD Articles 2.d and 2.e respectively (See Supra n65).

[74] See for instance, Leenes R. "Who Controls the Cloud?" (2010), Revista de Internet, Derecho y Política, 7. <http://www.uoc.edu/ojs/index.php/idp/article/viewFile/n11-leenes/n11-leenes-eng> accessed 25th March 2012.

[75] Opinion 1/2010 on the concepts of "controller" and "processor", 00264/10/EN, WP 169, (2010), 17 and 8. <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf>, accessed the 25th February 2012.

All the European-based cloud providers chosen for this analysis tend to describe themselves as data processors.[76] However, there are many cases where the cloud provider is more than just a mere processor[77].This is when the provider determines the "means of processing" such personal data. This could be for example, the case of cloud provider offering a storage services. If the provider would limit himself to this storage activity, its categorization as "processor" seems reasonable (as long as it stores personal data). However, if the provider would process the data for further purposes (for example, monitoring), it might be considered as controller of this part of the processing.

Note that in a previous opinion to the one just cited[78], the WP 163 considered Social Network Service providers (SNS) as data controllers. In order to justify such decision, the WP mentions some requirements[79] which Francois Gilbert considers common to SaaS providers. Thus, we presume that in his opinion, SaaS providers should be considered data controllers.[80]

Peter Hustinx, European Data Protection Supervisor, claimed the following "*Which role is played by cloud computing providers will need to be determined on a case by case basis, in view of the nature of the cloud services*".[81] From this we can deduce that the features of the specific relationship between the contracting parties are determinant to conclude if the provider is processor and likely controller. At this point, it is important to underline that a

---

Such opinion when defining the data controller claims; the possibility of pluralistic control *("which alone or jointly with others"*) and the essential elements to the controller from other actors *("determines the purposes and the means of the processing of personal data"*).

[76]For instance, Twinfield T&C expressely says that "*Twinfield will be the data processor and Subscriber will be the data controlle*r". Clause 15.5 (See Supra n12). Although the other cloud-providers do not express themselves as "processors", we deduce it from their T&C.

[77]Opinion 5/2009 on Online Social Network; 01189/09/EN, WP 163, (2009),1. <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_en.pdf>. Accessed 24th of March 2012.

[78] Ibid,5.

"*They provide the means for the processing of user data and provide all the "basic" services related to user management SNS providers also determine the use that may be made of user data for advertising and marketing purposes - including advertising provided by third parties."*

[79] Ibid.

[80]Gilber F "Cloud Service Providers as Joint-Data Controller" (2011) IT Law Group,9. <http://blogs.law.stanford.edu/bestpractices2011/files/2011/06/GILBERT-Cloud-Providers-as-Joint-Data-Controllers.pdf>. Accessed 24th of March 2012.

[81] Hustinx P. "Data Protection and Cloud Computing under EU law"(2010) European Data Protection Supervisor,3. <http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2010/10-04-13_Speech_Cloud_Computing_EN.pdf>. Accessed 26th February 2012.

provider may be considered as a processor and a controller, in relation to different purposes of the processing[82] and therefore be subjected to different obligations.

Regarding a standard cloud contract, we would strongly recommend the setting of a list explaining under which circumstances a cloud provider should be understood as controller and which are the duties for both parties.

At this point we would like to point out and briefly explain some circumstances under which cloud providers could be excluded from the DPD applicability.

As already mentioned in the first chapter[83], the current cloud-computing landscape is usually integrated by "chains" of services and providers. Thus, any cloud-provider (IaaS, SaaS or PaaS) can itself sub-contract a cloud service for providing its services. This situation presents problems when determining if the sub-contractor should be understood as processor of the first provider end-user data. The problem comes when the sub-contractor does not know which kind of data is operated by the first provider, either because it has no access to it, or because it is encrypted. The same problem arises when a cloud provider cannot access the data stored into a cloud equipment or software by an end-user or when such data is encrypted.

"*Under current laws, someone who stores personal data for a controller is a "processor" - even if the storage provider has no idea whether the data are "personal data" or not, and possibly even if the data are securely encrypted and it doesn't have the key"*[84]. This is due to the possibility of decrypting such data[85]. Just in case the data is strongly encrypted before its storage in the cloud, it would not be considered as personal data[86], due to the impossibility for the provider to know whether the data stored is "personal" or not. A similar trend is followed with regard to the providers' possibility to access the data stored.[87]

---

[82] See Supra n80, 8.

[83] See Supra n22.

[84] Hon K. "Who's responsible for personal data in cloud computing? You and your Saas, Paas and IaaS providers", (2011)COMPUTERWORLDUK, CloudVision. <http://blogs.computerworlduk.com/cloud-vision/2011/05/whos-responsible-for-personal-data-in-cloud-computing/index.htm>. Accessed 5th June 2012.

[85]Hon W. K., Millard C. and Walden I "The Problem of 'Personal Data' in Cloud Computing - What "Information is Regulated? The Cloud of Unknowing, Part 1", (2011) Queen Mary School of Law Legal Studies Research Paper No. 75/2011 ,25. <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1783577>.Accessed 5th June 2012.

[86] Ibid, 29.
"it seems the best way to try to ensure information stored in the cloud is not considered 'personal data' in the hands of the cloud provider is to encrypt it strongly before transmitting it for storage, also taking other technical and organizational measures such as securely storing the decryption key and strictly limiting access to it."

[87] Ibid, 34.
"the effectiveness of measures to prevent persons other than the user from accessing the user's stored personal data may affect whether the data are 'personal data' as regards those persons. Therefore, it seems that a key factor will be the

This is the case of Twinfield, which expressly claims that the provider has no knowledge of the content uploaded by end-users, and therefore, it does not accept any liability from the saved content. However the provider makes efforts to ensure the correct record of the content uploaded.[88]

Hereby, we would suggest to follow the proposal of Hon W. K. who claims that any Cloud-provider whose services are used as mere storage instruments (usually IaaS and PaaS), whether by end-users or other cloud-providers, should not be considered as processors (but as intermediate "host") of data, as long as they do not know that the data they store is "personal data" or have no access to it.[89] Otherwise cloud providers would be obliged to apply the "processor" obligations established in the DPD for "personal data", when they do not even know whether the data stored is personal or not.

B. Security measures:

Since the DPD establishes strict obligations on the data controller[90] who needs to know whether or not the security measures offered by the processor offer sufficient guarantees and ensure the compliance with those measures.[91]

However, the Directive leaves freedom to the Member States when implementing what should be understood by "*appropriate technical and organizational measures to protect data*".[92] Therefore, we find different security measures implemented throughout Europe, which means that not all the cloud end-users are protected at the same level, because not all the processors apply the same security measures when protecting the personal data processed. We personally find this situation very dangerous because we cannot forget that data controllers might find themselves liable by the processor acts or omissions when applying the DPD.

Coming back to the European-based cloud providers, we find the following scenario:

---

effectiveness of the cloud provider's access control system, which typically only allows authenticated and authorized cloud users to use a particular cloud account."

[88] Twinfield T&C, clause 12.7,12.8 and 12.9. (See Supra n12).

[89] Hon W. K., Millard C. and Walden I, " Who is responsible for personal data in cloud computing? The cloud of unknowing, Part 2", (2011) Queen Mary School of Law Legal Studies Research Paper No. 77/2011 ,29.
< http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1794130>. Accessed 5th June 2012.

[90] DPD articles 6, 7, 12, 10 and 17.1 (See Supra n65).

[91] Ibid, article 17. 2.

[92] Ibid.

Twinfield in its article 15.8 says *"Twinfield will take reasonable measures to protect the personal data saved or processed in the Webservice…will make reasonable effort to prevent unauthorized persons from accessing data of Subscriber. The information regarding these measures will be made available to Subscriber for inspection, to a limited and responsible extent, on Subscriber's request*". A later article specifies the characteristics of the location from where the Webservices are offered (including automatic back-up).

In the same way, Cloudee T&C specifies in its article 5.3 that the supplier will take reasonable steps to ensure that the customer's data is treated securely. However, no additional information is provided.

Similarly, CloudControl T&C on its article 14.3 affirms that all the technical and organizational measures to ensure the implementation of the German Data Security Law have been taken. Therefore, we see that the DPD has already been implemented by remitting to the Bundesdatenschutzgesetz, BDSG.[93] However, such national law does not specifically display how these measures should be implemented.

Switzerland does not belong to the European Union and the DPD is not applicable. The legislation applicable there is the Federal Act on Data Protection.[94] Such Act presents many similarities when talking about security measures of the data processing, which states: *"article 7.1: Personal data must be protected against unauthorised processing by appropriate organisational and technical means."*

Taking into consideration all these practical contracts, we see that cloud-providers mostly promise "reasonable" security systems to secure customers data and comply like this with the DPD. Thus we can see different levels of protection across EU. One effective solution to solve the just mentioned security problems would be in setting of a framework where technical and organizational measures are established in order to secure the data processed.[95]

A simple way to reach this type of security would be agreeing upon on the applicability of a Standard, like the ISO/IEC 27001.[96] The goal of the just cited standard is to "*provide a*

[93] Federeal Data Protection Act (BDSG), December 20, 1990 (BGBl.I 1990 S.2954), as amended by the law of 14 September, 1994 (BGBl. I S. 2325), section 9 and ANNEX <http://www.iuscomp.org/gla/statutes/BDSG.htm#9>. Accessed 26th of April 2012.

[94] FADP of 19 June 1992 (Status as of 1 January 2011) 235.1 <http://www.admin.ch/ch/e/rs/2/235.1.en.pdf>. Accessed the 2nd March 2012.

[95] Tightly connected to this issue is Hogan M., Liu f. and Sokol A. "NIST Cloud Computing Standards Roadmap" (2011), National Institute of Standards and Technology , special Publication 500-291,40. <http://collaborate.nist.gov/twiki-cloud-computing/pub/CloudComputing/StandardsRoadmap/NIST_SP_500-291_Jul5A.pdf>, which lists the major security objectives which should be implemented in cloud computing scenario. Accessed 21st February 2012.

[96] The ISO27001 certification process is deployed in the table 1 of the Annex 8. Such standard is usually fulfilled by the ISO/IEC 27002 or ISO/IEC 27005 which, respectively deploy control mechanisms to be implemented in the cases specified by the ISO/IEC 27001 and guidelines for information security risk management.
Links: ISO/IEC 27001 <http://www.27000.org/iso-27001.htm>

model for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an Information Security Management System".[97] Through this security model, organization security processes are analyzed and tested against the requirements set in the standard. Therefore, an independent auditor guarantees that the organization meets the security controls and activities put in place by ISO. In those cases, the company would deliver the audit certification to the customers who would be aware of the security controls carried out by the provider.

C. Geographical location of data and transfer

The DPD provides a regime for the transfer of data where companies are not allowed to transfer personal data outside the European Economic Area (EEA) to third countries not offering the same level of protection[98]. Although some exceptions[99] are set to this general rule, we will not enter into their analysis.

In the case of Twinfield, the location of end-user data is specified as follows; after being compressed and encrypted, it will be saved and processed in a country forming part of the EEA. However the country of process and storage is not specified. Moreover, when entering into the contract, end-users consent to transfers as required by applicable data legislation.

Cloudee differs from the scenario just explained, since its article 5.2, displays that through their consent, customers approve that their data may be transferred to third countries outside the EEA.

CoudControl does not make reference to this issue in the contract, but it is in its website where we can find that end-users' data will be stored and processed in Ireland.

CloudSigma specifies in its privacy policy that all the data is stored in Switzerland (base country of the cloud-provider). Additionally, it is said that end-users would receive a notice when information about them might be transferred to third parties (otherwise the transfer will not take place). This provision is the translation of the article 6.2b of the Swiss

---

ISO/IEC 27002 <http://www.27000.org/iso-27002.htm>
ISO/IEC 27005 <http://www.27000.org/iso-27005.htm>. All the websites were accessed the 24th March 2012.

[97] Cited extracted from "ISO 27000 Directory" <http://www.27000.org/iso-27001.htm>, accessed 24th March 2012. For further information about this standard, visit <http://www.27000.org/index.htm>.

[98] See Supra n65, article 25.

[99] Ibid, article 26.1.

FADP.[100] Indeed, alike to the DPD, the transfer of data is limited to countries presenting an adequate level of security; otherwise the previous consent of the end-user is required.[101]

We cannot forget that Switzerland does not form a part of the EU; hence different provisions from the DPD apply. Such circumstance is described in the privacy policy of the cloud-provider which says "*All data on virtual drivers remains on servers wholly owned and controlled by CloudSigma within the legal jurisdiction of Switzerland. If you are resident in the EU please note that the Personal Information and Virtual Drive Data you provide to CloudSigma are stored in Switzerland. The data protection laws of Switzerland differ from those of the EU and you expressly agree to such a transfer for the purpose of us providing you with the information and services you request."*[102]

Table 2

Europe Summary
• **Security measures:** The controller of the data is responsable for securing such data (even if it is processed by the cloud provider). Therefore, it has to ensure that adequate security measures are set in place by the provider. *Problem*: What should be understood by adequate security measures? Each Member State implemented the Directive in a different way, so it is a responsability of the end-user to know the location of the controller, and what security measures are in place. *Contracts in practice:* While all the providers claim that adequate security measures are in place to protect the data stored and secured, just some of them specified these measures. • **Geogregraphical location of data and transfer:** The DPD restricts the transfer of personal data outside the European Economic Area. Otherwise, transfers are just allowed to countries offering an adequate level of protecion when processing personal data (USA, by means of safe harbor, and Switzerland are deemed such countries). *Problem*: end-users need to know where their data is located and to which countries it might be transfered. *Contracts in practice*: in general we observe that all the contracts specify that the data is located in an EEA country (somethimes specified), and that the data transfers will be in accordance with the data protection legislation. (implementation of the Directive).

2.2 Intellectual Property Rights

As we already know, information in the cloud is in constant movement since end-users upload new content to the cloud. There is a question which should be clearly addressed in every T&C: who owns the data stored in the cloud?

[100] See Supran94.

[101] A.H. Schmidt "Cloud computing legal framework and privacy" (2011) Hacking,39. <https://communities.ca.com/documents/2231450/66169477/RWynn+-+Cloud+Computing+Legal+Framework+and+Privacy+-+Hakin9+May+2011.pdf> Accessed 26th of April 2012.

[102] CloudSigma Terms of Service <http://www.cloudsigma.com/en/platform-details/legal?t=2> Accessed 20th February 2012.

From an end-user perspective it is essential to make sure that all the data updated into the cloud remains under their ownership. Contracts need to make clear that no right is going to be acquired by the provider over the end-user data, and the opposite.[103]

When analyzing the contracts, we realize that not all of them approach IP rights in the same way.

For example, Cloudee in its article 1.5 expresses that all the property rights of the service belong to the supplier. However, nothing is said about the end-user property rights. A wider protection is held by Salesforce and Amazon. Both contracts expressly claim that any party obtains no right (including any related intellectual property right) over the other's contracting-party content.[104]

Contrary, from the provider perspective, it is interesting to make sure that the contract establishes the obligation for end-users to grant a license to the provider allowing this later to publish the end-user data.[105]

This is the case of CloudControl where, additionally to the information just cited, it is a end-user obligation to grant to the provider with: "*a worldwide, royalty-free, and non-exclusive license to reproduce, adapt, modify, translate, publish, publicly perform, publicly display and distribute such Application for the sole purpose of enabling CloudControl to provide you with the Services*"[106]. This fact would mean that the provider should be held as controller of the personal data covered by the License, since he will be the one deciding the means and purpose of such processing.[107]

We see that while some contracts just refer to the ownership of the IP rights, others go further and say that the contract includes the granting of a license in order to allow the provider to republish or modify end-user data when it may be necessary for the cloud computing service. Which is the general trend followed in every of the scenarios analyzed?

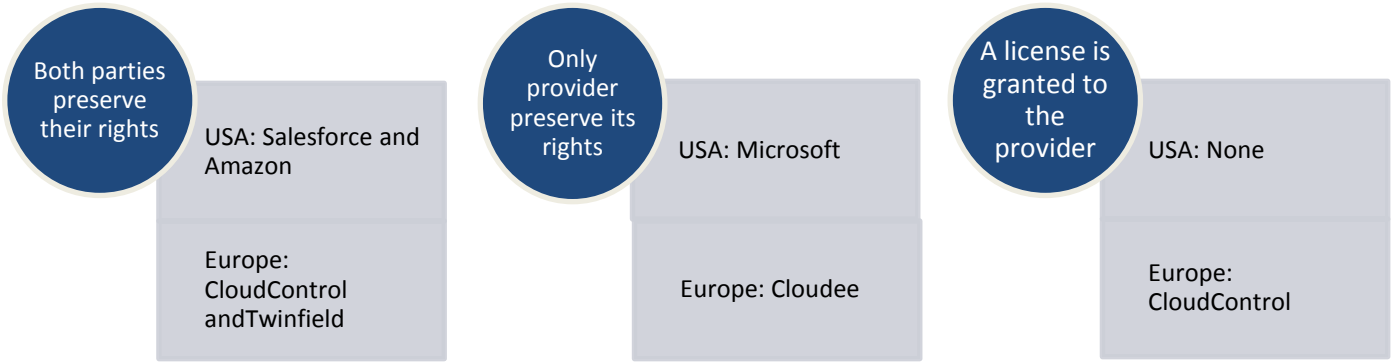
[103]JISC Legal Information "User Guide : Cloud Computing Contracts, SLAs and Terms & Conditions of Use" (2011) §2.2 <http://www.jisclegal.ac.uk/ManageContent/ViewDetail/ID/2141/User-Guide-Cloud-Computing-Contracts-SLAs-and-Terms-Conditions-of-Use-31082011.aspx>. Accessed 16th of February 2012.

[104] Salesforce Master Subscription Agreement, clause 7.4 (See Supra n11), and Amazon Web Services Customer Agreement, clause 8.1 (See Supra n13).

[105] See Supra n103.

[106] CloudControl T&C, clause 13.1 (See Supra n16).

[107] See Supra n82.



From the charts above we see that only SaaS providers make clear that any party will transfer no right to the other contracting party. Meanwhile, different strategies are followed by PaaS and IaaS providers. We consider necessary to make express mention to the fact that both parties will remain owner over their content, otherwise the provider could take over end-user content without being stopped for doing so. Additionally we see that just CloudControl (PaaS European-based provider) has opted for the granting of a license to the cloud-provider over end-user content. In this specific situation the provider may make profit from its end-user intellectual property rights. However, end-users should be those who will decide to whom they want to grant licenses.

2.3 Confidentiality and Disclosure

Contracting parties may have a special fear about the protection of certain kind of content such as: their data uploaded, but also trade secrets, businesses plans or any information or commercial value, which may want to be treated confidentially.

Due to the importance of the topic, all additional requirements regarding how this content is treated should be expressly defined in the contract.

Although all the contracts analyzed refer to this issue, cloud providers display different levels of protection with regard to this topic.

2.3.1 USA:

The scenario presented by US-based providers depicts different ways to secure confidential information, and the circumstances when this data can be disclosed vary among providers.

The most extreme positions and lowest protection for the end user can be found in the Amazon, where the duty of confidentiality by the provider does not exist. The agreement just makes mention to end-user obligation to keep the provider's information confidentially[108]. On the other hand, Microsoft and Salesforce expressly say that each party needs to keep the other's party confidential information.[109]

Amazon when addressing to the end-users' obligation not to disclose any provider's confidential information' it additionally expresses that this duty lasts for five years once the contract finishes, and reasonable measures should be taken by the end-user for protecting the provider's confidential information. Moreover, in the privacy policy, Amazon warrants that no content of the end-user will be disclosed without asking him for previous consent. This mechanic is called "pre-existing privacy notice". However, account or personal information of the end-user is disclosed when Amazon believes that this is appropriate to *"comply with the law; enforce or apply our Conditions of Use and other agreements; or protect the rights, property, or safety of Amazon.com, our users, or others. This includes exchanging information with other companies and organizations for fraud protection and credit risk reduction."*[110]

An intermediate position is presented by Microsoft which goes a bit further when protecting end-user confidential information, since the cases when end-users' content may be disclosed are narrower. Apart from the compel of information made by law, the Privacy Statement displays two other causes when Microsoft can disclose end users' information or content, being *"(b) protect the rights or property of Microsoft or our customers, including the enforcement of our agreements or policies governing your use of the Service; or (c) act on a good faith belief that such access or disclosure is necessary to protect the personal safety of Microsoft employees, customers, or the public*"[111]. Moreover, derived from the article 2.g T&C we see that end-users are responsible for protecting the confidentiality of any service associated with the agreement.

Contrary, Salesforce shows a higher protection. we can clearly see that a degree of care is taken by the provider (never less than reasonable care) to protect the confidential

[108] See AWS Customer Agreement, clause 13.1 (See Supra n13) .

[109] See Microsoft Online Subscription Agreement Clause 5 (See Supra n15).and Salesforce Master Subscription Agreement, clause 8.1 (See Supra n11).

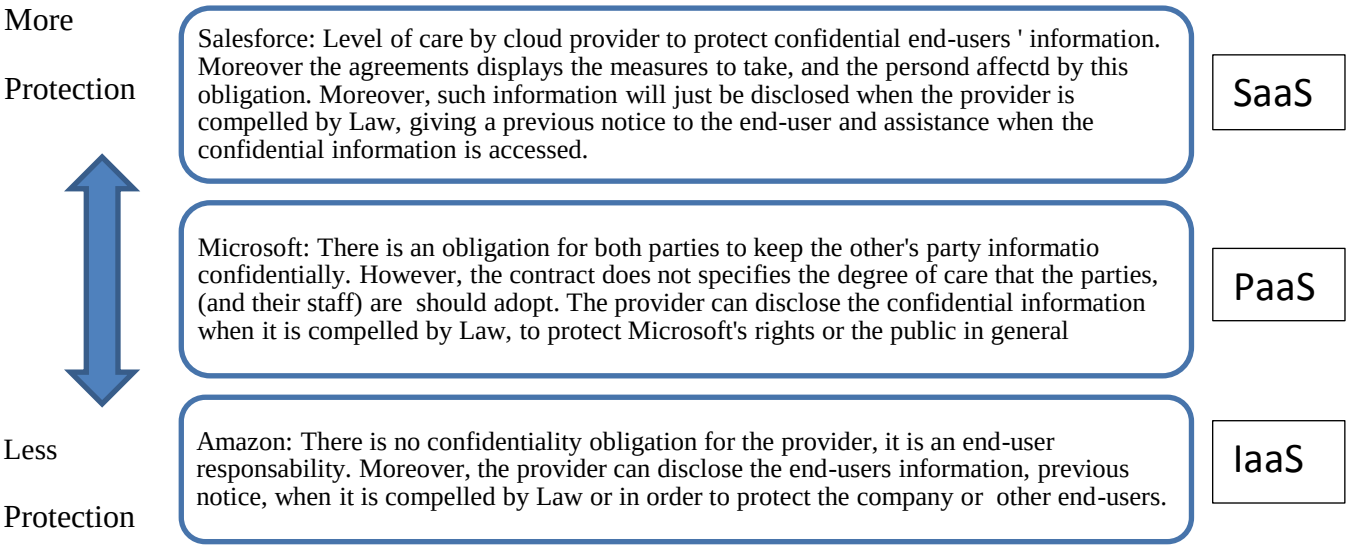
[110] "Amazon Privacy Notice Policy" <http://www.amazon.com/gp/help/customer/display.html?ie=UTF8&nodeId=468496>. Accessed 3rd March 2012.

[111] See Supra n61.

information. We find interesting the fact that this provider is the only one, who explains to whom this duty apply (employees, affiliate' employees, agents or contractors or either parties) and how (signing confidentiality agreements)[112].

Moreover, this provider may only disclose end-users' confidential information when they are legally compelled to do so, giving first notice to the customer to the extent permitted by law. Additionally, Salesforce will reasonably assist the disclosure of the information compelled by providing secure access.[113]

Table 3: Summary



We observe that the IaaS provider is the one offering the lowest level of protection since the provider is not obliged to keep end-users' data confidentially. These are these ones who need to take all the security measures they deem necessary to keep their data confidential.

2.3.2. Europe:

All the European based-providers' contracts selected claim a mutual obligation of confidential treatment of each-other's content. It is important to note that the DPD in its article 16 specifically claims the obligation to process personal data confidentially[114]. Such obligation

[112] Salesforce Master Subscription Agreement, clause 8.2 (See Supra n11).

[113] Ibid, clause 8.3.

[114] It seems that all the information which needs to be treated confidentially could fit within the meaning of personal data.

must include the behavior of the cloud organization's staff, but also end-user's employees[115]. In most occasions, this obligation for confidentiality lasts over a determinate period once the agreement is terminated. However, the cases when such confidential information may be discloses vary slightly from one provider to another.

Thus, Twinfield expresses that it shall disclose confidential information to "*employees, officers representatives or advisers*" needing it for the performance of the Agreement. Additionally, it shall also display it as response to any requirement made" *by law, court order or any governmental or regulatory authority*"[116]. However no measure to comply with such confidentiality obligation is detailed.

Cloudee claims that the provider can report to the authorities any conduct which, at its discretion violated applicable law. Besides, such disclosure can take place also in response to a request from law enforcement, a regulatory agency or a request in a civil action. In none of the just mentioned cases the notice to the customer is required. Additionally, the agreement sets the reciprocal requirement of confidentiality for one year once the contract finishes.[117]

The only provider making mention to the measures taken to keep end-users' data confidential, is CloudControl[118] which remits to the German Data Security Law that in its section 5 states "*Persons employed in data processing shall not process or use personal data without authorization (confidentiality) . On taking up their duties such persons, in so far as they work for private bodies, shall be required to give an undertaking to maintain such confidentiality. This undertaking shall continue to be valid after termination of their activity."*

From there we deduce that the personal will be required to sign some kind of confidentiality agreement or similar undertaking.

2.4 Warranties and Disclaimers

The contract needs to make clear which warranties can be received from the cloud provider all over the performance of the service.

2.4.1.USA

[115] See Supran65, article 16.

[116] Twinfield T&C, clause 15.3 (See Supra n12).

[117] Cloudee T&C , clauses 5.3, 5.4 and 5.6 respectively (See Supra n14).

[118] See CloudControl T&C. clause 14.3 (see Supra n16).

The general trend drawn by US-based providers is to limit the warranties as much as possible.

Indeed, from the three contracts analyzed, just two warrant the performance of the service in accordance with the specifications of the same; usually specified in the SLA.

Thus, Microsoft warrants the performance of the service as described in the SLA annexed to the contract, displaying also the remedies foreseen for the breach of such warranty.[119] Similarly Salesforce warrants the performance of the service in accordance with the user guide, claiming that the functionality of the service will not be decreased during the subscription term.[120]

Besides, the three contracts analyzed present a very broad disclaimer clause in which it is said that, apart from the warrantees mentioned above, the provider makes no warranties of any kind, and "*each party specifically disclaims all implied warranties, including any warranties of merchantability or fitness for a particular purpose, to the maximum extent permitted by applicable law*".[121]

A different strategy is held by Amazon, whose disclaimer clause expressly excludes any warranty, rejecting even its responsibility for the security, loss or damage of end-user or third parties' content.[122] Amazon Web Services are offered "AS IS", which means that the provider assumes no risks, excluding all liabilities where permitted by law [123]. In this case, end-users have the responsibility to adequate security of the service, data protection and backups.

2.4.2. Europe

Twinfield makes every effort to warrant that the service works properly. In order to ensure that, it specifies the objective measurement assessment. However, in a later stage it

[119] Microsoft Online Subscription Agreement Clause 6 (See Supra n15).

[120] Salesforce Master Subscription Agreement, Clause 9 (See Supra n11).

[121] Ibid.

[122] AWS Amazon Customer Agreement, clause 10 (See Supra n13).

[123] Vincent M. and Hart N., "Legal issues in the Cloud - Part 3" (2011) CIO. <http://www.cio.com.au/article/382652/legal_issues_cloud_-_part_3/>. Accessed 23rd April 2012.

claims that such warranty is just performed if the end-user performs a minimum system requirement. [124]

Additionally, the provider disclaims any error deriving from the network availability "*Twinfield does not warrant that Subscriber's use of the Webservice will be uninterrupted or error-free, nor that the Webservice will meet Subscriber's requirements; and is not responsible for any delays, delivery failures, or any other loss or damage resulting from the transfer of data over communications networks and facilities".*[125]

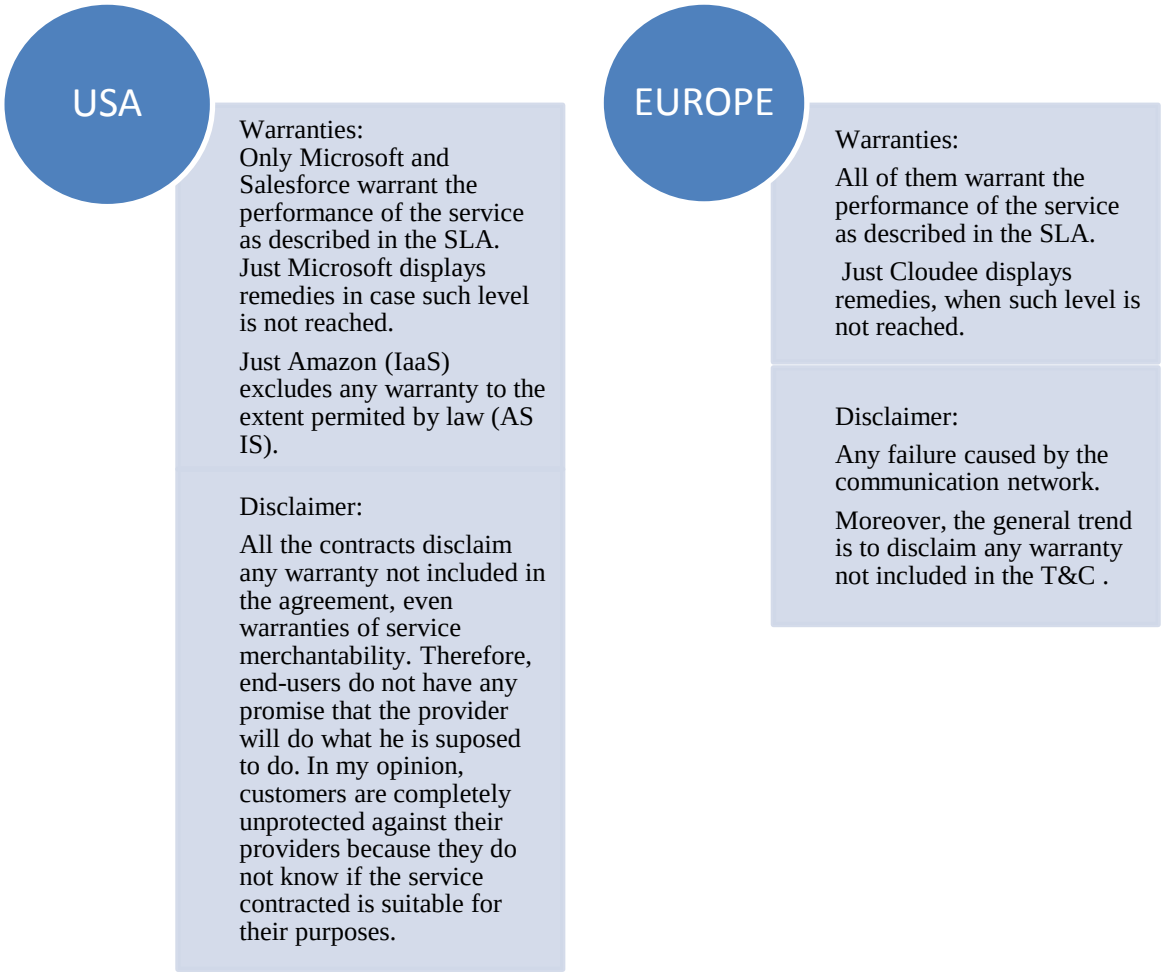
A similar protection is being provided by Cloudee[126], however in this second contract the provider makes available different alternatives to be taken when there is a fault or defect in the service, being the end-user who needs to choose the alternative which best fits his needs. With regard to the disclaimer, Cloudee adds to the one explained above, that any other warranties regarding third parties services, or other conditions not included in the agreement are equally disclaimed.

Table 4: Summary.

[124] Twinfield T&C, clause 19 (See Supra n12).

[125] Ibid.

[126] Cloudee T&C, clause 3 (See Supra n14).



Once again, when analyzing the contracts chosen, different levels of protection are displayed through the cloud provider contracts. However, it would be interesting to set a minimum level of protection. Thus, all the contracts should warrant that the performance of the service will be in accordance with the specifications of their SLA.[127]

2.5 Limitation of Liability[128]

[127] Note that SLAs cannot be standardized because each service present different features and characteristics.

[128] See Supra n9, 33-36.

As we will see, not many damages are covered by the cloud provider's liability clauses, and those covered, might be quite limited. The liability clause is an essential clause, since otherwise, end-users may not know what to expect from their provider, and when they are allowed to claim damages.

2.5.1. USA

US-based providers try to negate their liability as much as possible; therefore, they try not to be held liable for any damage. Despite the fact that all the contracts seen take the same approach towards this topic, some remarks need to be said though.

All the providers analyzed, exclude their liability for direct damages, to the extent permitted by Law. Moreover, they all claim that they will not be held liable for indirect, consequential, special or incidental damages, including among them, damages for loss of profits or revenues, business interruption or loss of business information.

Microsoft, claims that the provider remains liable up to a fixed amount of money. This amount of money will be the lowest to choose between the amount paid by the end-user during the term, or over the year before the filling of the claim. When the service is free, the liability is limited to five dollars.

However, such monetary restriction does not take place in four situations[129];

- When the damage derives from a provider's obligation titled "Defense of infringement. Misappropriation and third party claims"
- Damages awarded by Court for employee's or agent's negligence or misconduct
- Damages arisen from a breach of confidentiality from the provider's perspective
- Liability for personal injury or death due to providers', its empolyees or agents' negligence or misrepresentation.

Similarly, Salesforce restricts the amount of money constituting the indemnification to the lowest between five hundred thousand dollars, or the amount paid by the end-user in the twelve months before the incident; however no exclusion is set for this rule.[130]

[129] Microsoft Online Subscription Agreement, clause 8a (See Supra n15).

.

[130] Salesforce Master Subscription Agreement, Clause 11.1 (See Supra n11).

Amazon alludes at the same time to direct and indirect damages. Actually its liability clause sets a very broad range of exclusions, displaying that the provider will not be held liable for any damage (direct, indirect, incidental, special, consequential or exemplary), to the extent permitted by law[131]. Therefore, it will not be responsible for any compensation arising from end-user inability to use the services, cost of procurement of substitute goods or services; any investment made in connection with the agreement or the use of access to the service or finally, unauthorized access, alteration, damage, loss or failure to store customer's data.

Moreover, the amount of money composing the indemnification, in all other cases, will never be more than what the customer paid over the last twelve months before the claim was submitted.[132]

To finish with, there is an extra clause called "force majeure" destined to the exclusion of liability for both parties, when the damage is caused by the non-performance of their obligations caused by any cause beyond their control. Causes under such "uncontrolled facts" are commonly: natural disaster, war, explosion or other events for which precautions are not taken in the industry (for being not predictable). It is important to say that, since these services are deployed through the Internet, the interruption of the same would fit in those cases of force majeure. Such clause is present in all the contracts analyzed.[133]

2.5.2. Europe

On the other hand, European-based providers do not limit their liability in such way. Note that European-based providers cannot exclude their liability too far (when the end-user is a consumer; usually in SaaS and IaaS services) because they are subjected to Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contract. This directive indicates in its annex a non-exhaustive list of terms considered to be unfair.[134]

[131] Remember that its disclaimer is "AS IS"; therefore the provider excludes all its liability to the extent permitted by Law.

[132] AWS Amazon Customer Agreement, clause 11 (See Supra n13).

[133] Microsoft Online Subscription Agreement clause 10m ,Amazon AWS Customer Agreement clause 13.2 and Salesforce Master Subscription Agreement, clause 4.1 (b) (see Supra n15,13 and11 respectively).

[134] Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts *OJ L 095, 21/04/1993* <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31993L0013:en:HTML>. Accessed the 1st march 2012.

When talking about direct damages, European-based providers clearly state in which cases they are or are not liable. However, their approach to indirect damages is quite similar to the one held by US-based cloud providers.

CloudControl and Twinfield expressly mention the cases in which they can be held liable.[135]

The former limits its liability to predictable damages (caused intentionally or negligently) arising from defects of quality and title or infringement of contractual obligations. However, the limitations just explained are not applicable for the damage of life, body or health and product defects.[136]

The latter sets its liability in respect of any breach of Agreement, any use of the service by end-users, any service provided by Twinfield and any act or omission connected to the service. Like in CloudControl, the liability of Twinfield cannot be excluded or limited in certain cases; death or injury caused by the provider's negligence, fraud or fraudulent misrepresentation and finally, damage caused by any intentional or negligent action of Twienfield's managers. Moreover the liability to pay cannot be higher than the fees paid by the subscriber during the last twelve months preceding the damage.

When talking about indirect damages, Twinfied expressly stipulates its exclusion of liability for, among others, any loss of profit, loss of business or loss or corruption of data or information. Contrary, CloudControl does not address this kind of damages.

Cloudee excludes any loss or damage which may be suffered by the customer, directly or indirectly, if they fit in any of these categories "*a) special damage even though the Supplier was aware of the circumstances in which such special damage could arise; b) loss of profits; c) loss of business opportunity; d) loss of goodwill; e) loss of data.*"[137]

Therefrom we see that the cases under which the provider could be held liable are no expressly described. It is remarkable how low the amount of money for which the supplier is held liable is: the indemnification cannot exceed the amount the payment made by the end-user within the last three months of service.

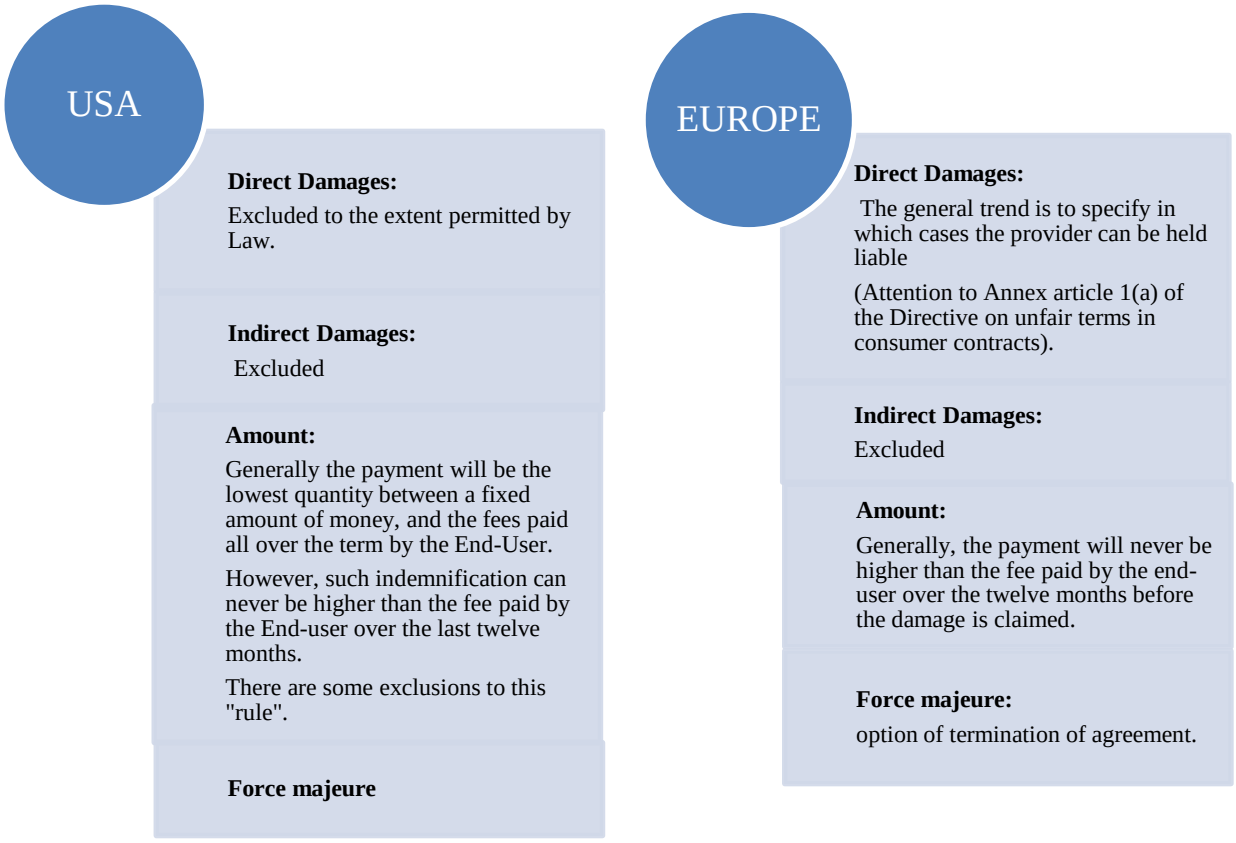
[135] CloudControl Terms of Service, Clause 15 and Twinfield T&C clause 6 (See Supra n16 and 12 respectively).

[136] Following therefore the limitation of liability detailed in the Annex article 1(a) of the Directive on unfair terms in consumer contracts (See Supra n134).

[137] Cloudee T&C, clause 3 (See Supra n14). Remember that both cloud-providers offer IaaS services, and therefore their liability is extremely reduced.

Moreover, the three providers mention the "force majeure" clause. If the delaying event takes more than 60 days, Twinfield gives the option to terminate the agreement after written notice to the other party.[138]

Table 5: Summary



2.6 Indemnifications:

The contract should make clear in which cases the end-user can be obliged to indemnify the provider and vice versa.

As we will see, all the studied contracts make reference to the cases when end-user need to indemnify their provider. Mostly all the agreements face the issue at the same level. Just some exemptions were found.

Not surprisingly, the references to indemnification by the provider to the end-user are quite few and restricted. We believe that end-user rights are too limited; therefore cloud

[138] Twinfield T&C, clause 10 (See Supra n12).

customers are left unprotected against their provider. It is remarkable to say that just some US-based cloud providers make reference to this topic.

2.6.1. Indemnification by the end-User

End-users are obliged to indemnify their provider when certain circumstances occur.

Almost all the contracts analyzed make mention to the end-user obligation of indemnifying their provider when this latter is sued by third parties who claim damages:

- On their intellectual property rights derived from the content held by provider on the end-user's behalf,
- Derived from the use of the service made by the end-user,
- Breach by the end-user of the Agreement or applicable law.

At this point we find interesting to comment that only Cloudee extends the indemnification causes to "*any act or omission by the Customer*"[139]. Furthermore, apart from the general settings just mentioned, Amazon incorporates another cause triggering indemnification by end-users, such as "*mere dispute of end-user with other parties*"[140] . However, this clause seems too burdensome for end-users who might be obliged to indemnify their provider even when the "dispute" does not arise from any act or omission attributable to them, but to the other end-user involved in the dispute.

When any of the just cited situations take place, all providers agree upon the fact that the indemnification should cover the damages, attorney fees and any costs approved by the Court. Additionally, all providers, apart from Twinfield, set that before the indemnity is required by the provider, the end-user would be given a notice of the suit against him.[141]

Just two remarks are interesting at this point. The first refers to the non-existence of such clause in the CloudControl terms of service, since the effect for any of the conducts mentioned above would be the termination of the contract (Remember that the service offered by CloudControl is free of charge).

---

[139] Cloudee T&C clause 6.1 (See Supra n14).

[140] AWS Amazon Customer Agreement, clause 9.1 (See Supra n13).

[141] Cloudee T&C, clause 6 (See Supra n14), Microsoft Online Subscription Agreement, clause 7.e (See Supra n15), Salesforce Master Subscription Agreement Clause 10.2 (See Supra n11) and AWS Amazon Customer Agreement, clause 9.2 (See Supra n13).

Additionally, we find interesting to point out that while all US-based providers give end-user the sole control of the defense[142], the only European one making mention of this issue reserves its right to assume the defense and control of the matter, at the end-user expenses.[143]

2.6.2. Indemnification by the cloud provider

Few providers have clauses dealing with the topic of indemnification to the end-user of the service.

Actually, from the contracts analyzed, just two approach this topic.

Salesforce sets that the provider would defend the end-user from any demand or proceeding against this later by a third party claiming an infringement of intellectual property based on the use that the end-user made of the service.[144]

Similarly, Microsoft seems to base the indemnification by the provider on a similar matter; infringement of a third party´s intellectual property by the product (or service). However, Microsoft specifies that the indemnification is limited and just granted as far as the claim is not based on some aspects detailed in the agreement.[145]

In both cases, the payment by the provider is subject to the fulfillment of some conditions "sine qua non", for the indemnification to take place. These requirements consist of taking control of the defense by the provider and providing reasonable assistance when the claim is being defended. Moreover, both providers can, once they have knowledge of the infringement; allow continuing use of the service (through a license), modify it, replace it or terminate the agreement.

The indemnification, in both cases, is the same as the one explained above.

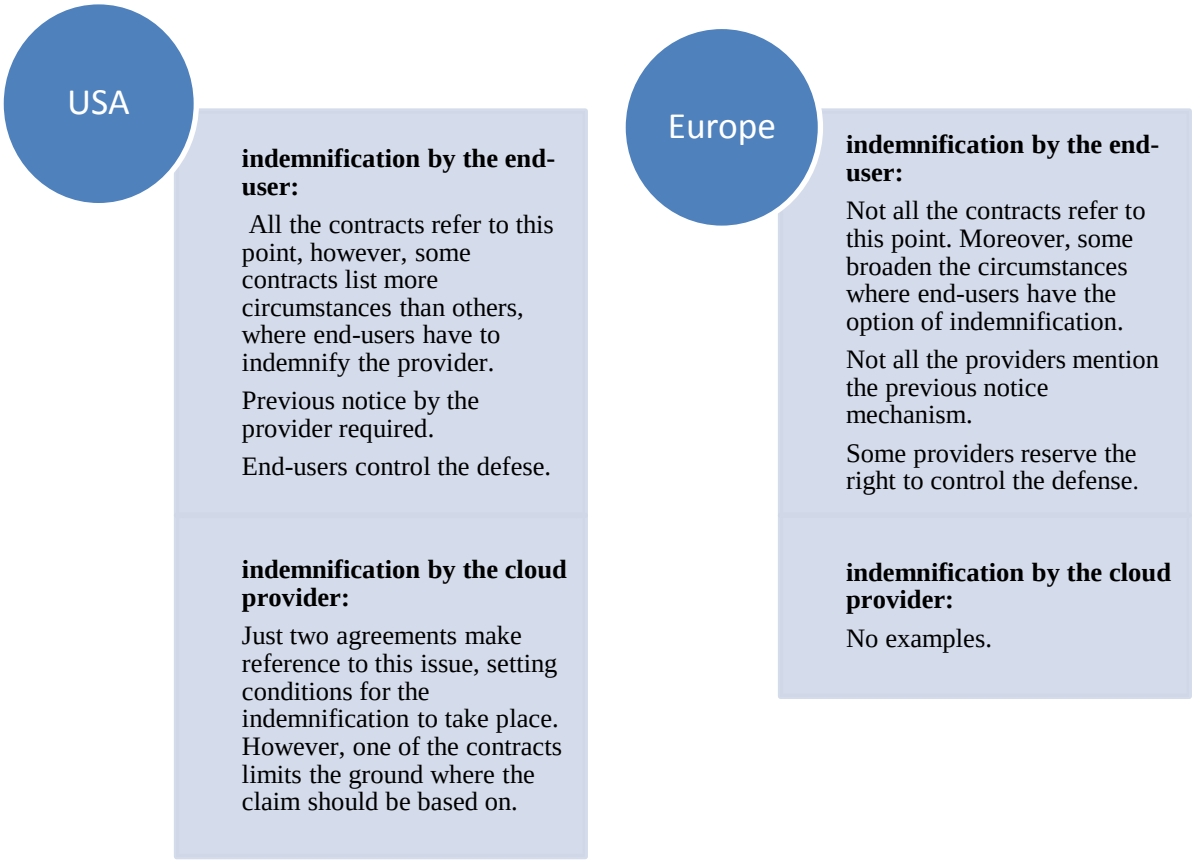
Table 6: Summary

[142] Microsoft Online Subscription Agreement, clause 7.e (See Supra n15), Salesforce Master Subscription Agreement Clause 10.2 (See Supra n11) and AWS Amazon Customer Agreement, clause 9.2 (See Supra n13).

[143] Cloudee T&C clause 6.1 (See Supra n14). Note that in this case, end-users need to provide reasonable assistance during the defense is taking place.

[144] Salesforce Master Subscription Agreement, clause 10.1 (See Supra n11).

[145] Microsoft Online Subscription Agreement, clauses 7.a and 7.b (See Supra n15).



2.7 Law and Jurisdiction

When talking about applicable Law different doubts arise. It is not clear whether the relevant jurisdiction should be the one, where the provider is based in, established or the one where the end-user has its domicile.

This clause is of extreme importance, especially for end-users, because if the applicable Law is not their national one, they might see themselves involved in a foreign jurisdiction and language.

Almost all the contracts studied claim that end-users agree, when signing the agreement, that applicable Law in case any conflict arises will be the national one where the provider is based in, or in case of the US-based cloud providers the law of the State where the provider is based in.

Just two annotations must be highlighted.

Firstly, just Salesforce makes available a table where it displays the correspondent applicable Law and Jurisdiction in function of the end-user domicile.[146] And secondly, Twinfied (Dutch cloud provider), claims in its English website, that any dispute or claim shall be governed by the laws of England and Wales.[147]

Referring to the jurisdiction, the Courts of the country which national law is applicable to the disputes between contractual parties shall resolve such claims in practice.[148]

At this point, we find two different paths. While mostly all agreements say that the jurisdiction set just above is binding, others, such as Cloudee, say that the jurisdiction named is non-exclusive.[149]

So basically, while the vast majority of cloud providers specify the law applicable and the jurisdiction, which must have knowledge of the issues that may arise between both parties, just few agreements leave open this issue. However not-binding options seem interesting, because they allow end-users to bring disputes within their jurisdiction, therefore making the clause written by Cloudee the most appropriate one from the end-user perspective.

2.8 Termination[150]

All the contracts analyzed seem to follow a similar structure when facing this topic.

2.8.1 Term

Most of the studied T&Cs start setting up the moment when the agreement begins and its duration, which commonly will last until one of the parties terminates it, or the subscription to a service expires. In this second case, the method to renew the subscription is explained.

[146] Salesforce Master Subscription Agreement, clause 13 (See Supra n11).

[147] Twinfield T&C clause 11.11 (See Supra n12). Note that in its Dutch website, the relationship between parties is governed by the Dutch law, and the Amsterdam District Court has exclusive jurisdiction.
We found this fact relevant because the other European-based providers, such as CloudControl, do not make differentiation about the applicable law in their different T&C language versions.

[148] In the case of US-based providers, the contract specifies the city where any claim needs to be brought.

[149] Cloudee T&C clause 14.1 (See Supra n14)

.

[150] See Supra n103, §2.17

2.8.2 Ways to terminate

At this point we need to differentiate the called termination "for convenience" from the termination "for cause".

The first one refers to the possibility of terminating the agreement for any reason (when a minimum period of time has passed), always that a notice is given in advance and the service's account is closed by the mechanisms provided. All the providers offer such possibility to both parties.

Termination for "cause" sets the possibility for both parties to finish the agreement at any time, only under determined circumstances and previous notice given to the other party. The basic causes refer to breach of agreement or no paying off debts.[151]

Additionally, some contracts refer to causes allowing the provider to terminate the contract, for example, for compliance of the Law or when it ends the relationship with a third-party provider of software or technology needed to provide the service.[152]

We find this possibility very reasonable, because otherwise cloud provider would remain obliged to comply with the agreement, when the performance of the same turns impossible for causes not directly attributable to them.

It is noteworthy that just Salesforce mentions the refunds or payments needed to be done to the other party once the termination takes place for cause.[153]

Finally, CloudControl claims that the contract may be terminated without prior notice or reason, by ending the use and deleting the data. It seems that when the services are free, no requirements are needed to terminate the contract, since the cloud provider can terminate it without formalities.[154]

2.8.3 Effects

[151] Some cloud providers broad the causes of termination. This is the case of Twinfield, which in is T&C clause 9.3 (d) to (j) mentions additional causes (See Supra n12).

[152] This is the case of Cloudee T&C clause 4.3(See Supra n14) , Microsoft Online Subscription Agreement clause 4.f (See Supra n15) and Amazon Web Customer Agreement clause 7.2 (ii) (See Supra n13). The main difference among them is that some providers require notice to the end-user, while others do not even mention such notice.

[153] Salesforce Master Subscription Agreement, clause 12.4 (See Supra n11).

[154] CloudControl T&C, clause 3 (See Supra n16).

While the main effect of the termination is that all the rights given under the agreement expire, other issues need a more detailed explanation. For instance, what happens with the end-users data once the contract is finished? This issue is of vital importance since end-users might be concerned about the way in which their data is going to be reverted and the time the provider may keep it, since the user may want to transfer his data or application to another provider.[155].

At this point we find differences between the two scenarios studied.

US-based providers offer a wide range of solutions. Some suppliers give their end-users the option to choose, within 90 days, between the deletion and the retention of their data, in order to give them the option to extract it.[156] Other providers claim that the end-user has 30 days to download his data in a file, after such period the data will be deleted.[157] Contrary, Amazon expressly says that the data will not be erased after the contract ends; however the customer can retrieve his data if he has paid a charge for any post-termination use and all other due amounts.[158]

For the European-based providers the situation is different.

Thus, in the T&C of Twinfield we see that the subscriber can request all the copies of its data (in a file format) to be reported after having paid a fee, however, such data was previously encrypted and the provider does not have the obligation of converting the data provided.[159]

No references to this issue are made in the other two agreements analyzed.

Moreover, no quote is made to "data portability" so we presume that it is not restricted. Otherwise the cited contracts would present a feature punishable by European competition law. "*Moreover, were a service provider to include in its standard terms and conditions, conditions that constrain a customer from porting, replicating or backing-up data, this would raise concerns from a competition law as well as a consumer protection perspective. Such terms may be deemed to be in breach of competition law if they either are not necessary for providing the service, result in barriers to entry, distort competition and harm consumers".*[160]

[155] It is important to mention that none of the contracts analyzed make mention to the "change of provider", existing therefore the possibility for the end-user to be locked-in to the cloud-provider.

[156] Microsoft Online Subscription Agreement, clause 4.e (See Supra n15).

[157] Salesforce Master Subscription Agreement, clause 12.5 (See Supra n11).

[158] AWS Amazon Customer Agreement, clause 7.3 (See Supra n13).

[159] Twinfield T&C clause 21.2 (See Supra n12).

[160] See Supra n22, 25.

Therefore, data portability should be enforceable from a competition Law perspective.[161]

2.9 Monitoring by provider[162]

End-users are also concerned about the monitoring, which their cloud provider may perform. Indeed, customers are worried about the use that providers can make of their data. However, not all the suppliers follow the same path.

Hence, US-based providers such as Microsoft and Amazon held in their privacy statements details that personal end-user's information may be used in order to improve the service or the organization's needs[163].

Contrary, a different trend is followed by Cloudee which states that end-users data may be processed "*for purposes such as internal statistics, commercial sale and promotion"*[164] in a anonymised form. Similarly Twinfield claims that it is allowed to use the end-user data, in anonymous form, for strict statistical purposes, being therefore allowed to monitor the traffic data for the functioning of the service. [165]

At this point It is important to mention that the monitoring can be done through the use of cookies. From the Article 29 WP 56 we see that cookies can be considered as "personal data", since they identify an IP address which allows its personalization[166]. Hereby we see that these two European-based cloud providers seem especially careful when determining that they will only monitor data in an anonymous way. Otherwise, they would be considered as data controllers with regard to data collected through the use of cookies, since they would be deciding about further use of such data. Therefore, through the anonym use of data, they would not be controlling personal data, avoiding like this the strict obligations which the DPD establishes for data controllers.

---

[161] Ibid, "*According to the Commission, an individual should have the right to withdraw his own data from an application or service and transfer such data into another application or service, as far as this is technically feasible".*

[162] See Supra n9§4.11.

[163] See Supra n61, clause "support services" and Supra n110, respectively.

[164] Cloudee T&C clause 5.5 (See Supra n14).

[165] Twinfield T&C clause 12.16 (See Supra n12).

[166] Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites, 5035/01/EN/Final, WP 56(2002),10. <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2002/wp56_en.pdf>. Accessed 6th June 2012.

The only European-based provider making reference to the use of cookies for determining how end-users use the website is CloudControl. In its Privacy Policy the provider claims that end-users are awarded that certain information may be collected through the use of "cookies". Additionally it is said that the information generated by these cookies will be anonymized before being sent to the Google analytics provider in the USA. However, end-users are free to refuse such cookies by setting their browser. So basically, even if the data collected by the provider would not be considered as personal, end-users are still free to refuse such cookies.

To sum up we see that US-based providers tend to monitor their users in order to improve the service, while European ones refer to improvement of services and mere statistical analysis through monitoring of anonymous data.

CHAPTER THREE: Legal framework to be fulfilled in the standard contract.

The aim of this chapter is to give a brief overview of the legal framework that the contract we will later recommend in the fourth chapter should comply with. Since the contract we propose would try to respond to the already named "new cloud computing strategy for Europe", it will need to meet with all the requirements set all over the European Directives (for instance, DPD or eCommerce Directive) applicable to cloud computing.

Furthermore, as natural persons can also be end-users', the four chapter should present a contract in accordance with the consumer laws.

3.1 Data Protection.

As already explained in the second chapter, cloud providers are obliged by the DPD when processing personal data, which may also involve businesses' information likely to identify a person[167].

As several aspects regarding the DPD applicability have been widely explained all over this thesis, we will not give further explanations.

However we would like to point out some general aspects of the Directive, as a brief summary of the findings we came up with over the contracts' comparison:

- The article 4.1 c establishes that the DPD is applicable to non-European cloud providers processing and controlling personal data through the use of equipment (such as data centers of cookies placed in a end-user's hard disk) situated within a Member State.
- Controllers need to put in place stricter security measures implementing "*appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access*" [168] and are likely to be held liable for processor's omissions and acts. Therefore, cloud providers try to circumvent all situations which would qualify them as data controllers. For example, they anonymize the data they collect for the monitoring of their services and thus avoid the applicability of the DPD with regard to the data they collect.

[167] See Supra n66.

[168] Article 17.1 DPD.(See Supran65).

3.2 Electronic Commerce Directive

Contrary to the sub-question just explained, The Electronic Commerce Directive[169], does not show any problem with regard to its applicability by cloud computing providers since cloud computing services seem to fulfill all the requirements of "information Society services".[170]

This directive sets an intermediary liability regime, distinguishing among "mere conduit", "caching" and "hosting" providers[171]. Cloud providers, are likely to fit under this last category[172], and therefore will not be held liable for any damage or infringement triggered from illegal content they hold in their servers on end-users behalf, as long as they do not have knowledge of its unlawful character[173] .Note that the eCommerce Directive expressly excludes the DPD, so the intermediary liability it proposes does not cover personal data. Moreover, the eCommerce Directive does not oblige providers to monitor their customers[174]. Thus, their liability is restricted to a "notice and take down" procedure.

[169]Directive 2000/31/EC of The European Parliament and of The Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce)" OJ L 178/1, 17.7.2000 <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:178:0001:0016:EN:PDF>. Hereinafter eCommerce Directive. Accessed 10th April 2012.

[170]We find the definition of "Information Society services" in the 98/48/EC Directive amending the Directive 98/34/EC :

ªserviceº, any Information Society service (ISS), that is to say, any service normally provided for remuneration, at a distance, by *electronic means and at the individual request of a recipient of services.*

For the purposes of this definition:

- ªat a distanceº means that the service is provided without the parties being simultaneously present,
-ªby electronic meansº means that the service is sent initially and received at its destination by means of electronic equipment for the processing (including digital compression) and storage of data, and entirely transmitted, conveyed and received by wire, by radio, by optical means or by other electromagnetic means,
- ªat the individual request of a recipient of servicesº means that the service is provided through the transmission of data on individual request.

.

[171] For further information see Jasper P. Sluijs, Pierre Larouche and Wolf Sauter "Cloud Computing in the EU Policy Sphere" Tilburg University. TILEC Discussion Paper, DP 2011-036 (2011), 35. <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1909877>. Accessed 10th April 2012.

[172] Ibid.

[173] See Supra n169, article 14.

[174] Ibid, article 15.1.

Additionally, this Directive establishes in its article 15.2 the possibility for Member States to enforce retention obligations to ISS providers offering storage services *"by requiring them to record the IP addresses used by their services' users"*[175].

This means that, even if cloud providers are not understood as Electronic Communication Services (and therefore not obliged to retain data) [176], Member States may still require the storage services providers' to retain certain end-user's data (IP addresses).

Note that depending on the service offered, the obligation to secure this non-personal data will rely either on the provider or end-user[177]. Hence, the standardization of these measures is not possible, we will not introduce this aspect in the standard contract.

3.3 Consumer protection

As already pointed out several times, end-users can also be personal consumers, and therefore, the contract we will display in the next chapter should be drafted in accordance to the European consumer laws.

However, the legislation addressing to this issue seems quite fragmented, because not all Directives relating to consumers are applicable to cloud computing. For instance, cloud services are excluded from the Sales' Directive scope (sale of consumer goods and associated guarantees), thus, there are certain rules which do not apply to them (for instance, the rules of non-conformity, legal guarantee and remedies).[178]

What rules should be implemented into the proposed contract?

---

[175] Moiny, J.P. "Are Internet protocol addresses personal data? The fight against online copyright infringement" (2011), computer law & security review,350. <http://alexandrie.droit.fundp.ac.be/GEIDEFile/6830.pdf?Archive=192885791006&File=6830_pdf>. Accessed 22nd May 2012.

[176] In accordance with the article 6 of the DRD, cloud providers offering electronic communication services, should retain the data no less than six months and no more than two years from the date of the communication.

Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ L 105, 13.4.2006. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF>. Accessed 7th March 2012. Therefrom Data Retention Directive (DRD).

[177] See sub-question 1.2.4

[178] For more information check: <http://europa.eu/legislation_summaries/consumers/protection_of_consumers/l32022_en.htm>.Accessed 4th June 2012.

Consumers are protected through the Unfair Terms Directive[179]. This Directive sets some guidelines and limits in order to avoid *"imbalance in the parties' rights and obligations arising under the contract, to the detriment of the consumer*"[180], when the clauses have not been negotiated individually. In order to give further guidance, the Directive displays an Annex to its article 3 containing a *"non-exhaustive list of the terms which may be regarded as unfair*"[181].

From this list we see some limitations which directly affect the providers' liability and disclaimer[182], termination of the agreement[183], warranties[184] and the choice of legal action or remedy to take[185]. All these aspects will be introduced into the model contract.

3.4 Electronic Communication Services (ECS).

.At this point of the analysis, it is important to mention two Directives of vital importance within the cloud computing scenario. The first one is the 2002/58/EC Directive[186], amended by the 2009/136/EC Directive[187], which sets some extra obligations for "*publicly available electronic communications services in public communications networks in the Community*"[188], mainly being;

[179] See Supra n134.

[180] Ibid, art 3.1.

[181] Ibid, art3.3.

[182] See Annex (1 a) to the article 3.3.

[183] Ibid, Annex 1d, 1f, 1g and 1o.

[184] Ibid, Annex 1m

[185] Ibid, Annex 1q.

[186] Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector. of the European Parliament and of the Council of 12 July 2002 (Directive on privacy and electronic communications), OJ L 201/37 31.7.2002 <http://www.aedh.eu/plugins/fckeditor/userfiles/file/Protection%20des%20donn%C3%A9es%20personnelles/Directive_EC_2002-58-_-_eng_.pdf>. Accessed 23rd February 2012. Hereinafter ePrivacy Directive.

[187] "Directive 2009/136/EC of The European Parliament and of The Council of 25 November 2009 amending Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws", OJ L 337/11 18.12.2009 . (Text with EEA relevance) < >. Accessed 23rd February 2012. Hereinafter "cookie Directive". This Directive required national Laws to implement the text by June 18, 2011. However, such deadline was wider to the 26th May 2012.

[188] Ibid, Article 3.

-security measures when processing personal data (article 4.1)[189],

- notify the end-users about the security breach risks (article 4.3) and

- obligation to ask end-users their prior consent for collecting information through cookies (article 6.3).[190]

Additionally, on the 15th March 2006 the European Council and the European Parliament adopted a directive on the retention of traffic and location data[191]. Such directive requires providers of publicly available ECS or of public communications networks to retain traffic and location data of legal entities and persons (not the content of the communication itself). The aim of this directive is to make available such data to the correspondent national authorities for the purpose of investigation, detection and prosecution of serious crimes[192]. The obligations that the DRD establishes for providers are mainly;

- the fact of retaining this data (article 6 in connection with article 12) and

- setting of a minimum security requirements (article 7).[193]

Due to the obligations which these Directives impose to ECS providers, it is necessary to consider whether cloud computing providers should be understood as such, and therefore obliged by these Directives.

Answering the above question turns to be a difficult issue, since the definition of "electronic communications services"[194] seems quite confusing[195] and do not perfectly fit within the services offered by cloud providers. It is true that we cannot understand cloud

[189]The security measures deployed in this article do not preclude the application of the ones required by the DPD.

[190] This last requirement seems especially important when talking about monitoring by provider.

[191] See Supran176.

[192] Ibid Articles 1 and 2.

[193] These security measures are enforceable without prejudice to the provisions established within the DPD and the ePrivacy Directive.

[194]Hereinafter ECS. Definition found at the Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services, OJ L 108/33 24.4.2002, article 2 (c). <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:108:0033:0033:EN:PDF>. Accessed 7th March 2012. Hereinafter Framework Directive.

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

[195] For further information see Supran171, 27-31.

providers outside the scope of this definition with regard to the exclusion of "*services providing, or exercising editorial control over, content transmitted using electronic communications networks and services"*[196] found in the definition. However, cloud providers do not always see themselves *"wholly or mainly in the conveyance of signals on electronic communications networks*"[197,198].

In its opinion 113 (2005), the article 29 WP tried to clarify the meaning and scope of ECS and claimed that, in the case of the Internet, ECSs should be limited to "*access provider and one-to-one communication (e-mail services, voice over IP) is necessary"* [199]. Therefrom we deduce that, as long as cloud providers give "access "[200] to their services, which as we already said, could be described as ISSs, they could be covered by the ECS definition. However, such "access" is not provided by the cloud-provider itself but by the ISP which is "*sending and receiving signals on the network"*[201]. From here we understand that ISPs are those which should be understood as "access provider", meanwhile cloud-providers should be

[196] See Supran194.

[197] Ibid.

[198] The definition of "electronic communication network" can be found in the article 2.a of the Directive 2009/140/EC of The European Parliament and of The Council of 25 November 2009, amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, OJ L 337/37, 18.12.2009. < http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0037:0069:EN:PDF>. Accessed 21st May 2012.

"electronic communications network" means transmission systems and, where applicable, switching or routing equipment and other resources, including network elements which are not active, which permit the conveyance of signals by wire, radio, optical or other electromagnetic means, including satellite networks, fixed (circuit- and packetswitched, including Internet) and mobile terrestrial networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable television networks, irrespective of the type of information conveyed;'

[199] "ARTICLE 29 Data Protection Working Party" WP 113 (2005),8. <http://www.edri.org/docs/Art29-WP113en-Data_Retention_Oct2005.pdf>. Accessed 12th of February 2012.

[200] The definition of Access is to be found in the article 2.a of the 2009/140/EC Directive amending the 2002/19/EC Hereinafter Access Directive.

'(a) "access" means the making available of facilities and/or services to another undertaking, under defined conditions, on either an exclusive or nonexclusive basis, for the purpose of providing electronic communications services, including when they are used for the delivery of information society services or broadcast content services. It covers inter alia: access to network elements and associated facilities, which may involve the connection of equipment, by fixed or non-fixed means (in particular this includes access to the local loop and to facilities and services necessary to provide services over the local loop); access to physical infrastructure including buildings, ducts and masts; access to relevant software systems including operational support systems; access to information systems or databases for pre-ordering, provisioning, ordering, maintaining and repair requests, and billing; access to number translation or systems offering equivalent functionality; access to fixed and mobile networks, in particular for roaming; access to conditional access systems for digital television services and access to virtual network services.';

[201] See Supra n171,27.

understood as ISP's end-users[202]. Cloud providers could, nevertheless be described as "associated services"[203] and be therefore covered by the Framework Directive.

However, from a hearing performed by the European Commission[204] we read the following:

> "*Cloud services can be delivered either on a standalone internet basis (with no link to access components), or in a bundle with a dedicated access service, or through subscription to an ISP (IT plus network) – but in each case they are distinctively information society services which fall outside of the telecoms remit. "*

From above we deduce that not all the cloud services (SaaS, PaaS and IaaS) are delivered in a same way, and therefore, while some of them could fit within the framework directive scope due to their "access component", others remain outside. Hence, while some services could fit within the meaning of ECS, others cannot.[205] Thus, depending on the services offered, some cloud providers could see themselves subjected to both, the ePrivacy Directive and the DRD.

This idea is also supported by a selected industry group which in recommendation paper on how to best approach the new cloud computing strategy for Europe, claimed the following "*... electronic communication services, ...excluding most cloud providers ...*"[206]. Once again, we see that not all the cloud providers overlap with the definition of ECS.

Due to interpretation problems derived from the wording of the Framework directive, national legislators or data protection authorities should clarify its scope. Moreover, the directive could be implemented differently across the Member States, thus entities covered might not be the same in all countries.

Since the aim of this Master Thesis is to offer a base standard contract for cloud computing services, we will not introduce any reference to ECS providers' obligations into the

---

[202] Ibid,28.

[203] Article 2 (ea) of the 2009/140/ EC Directive, amending the Framework Directive.

[204] "Hearing with Telecommunication and Web Hosting Industry ",Commission of the European Communities, Information Society & Media Directorate-General, Software & Service Architectures, Infrastructures and Engineering Unit (2011),3. <http://ec.europa.eu/information_society/activities/cloudcomputing/docs/hearingreport-telecomsv2.pdf>. Accessed 22nd May 2012.

[205] To the same conclusion came Pavel B. V. in her Master Thesis "Cloud Computing and The Regulatory Framework for Telecommunications and Information Society Services" (2012) Tilburg University, 37-45. <http://arno.uvt.nl/show.cgi?fid=121935>. Accessed 2nd June 2012.

[206] Industry Recommendations to Vice President Neelie Kroes on the orientation of a European Cloud Computing Strategy (2011),5. <http://ec.europa.eu/information_society/activities/cloudcomputing/docs/industryrecommendations-ccstrategy-nov2011.pdf>. Accessed 6th June 2012.

contract proposed. Otherwise, stricter obligations for cloud-providers not offering ECSs would be generalized.

CHAPTER FOUR: Proposal of European Standard Contract

In the present chapter we propose an "add-on" standard contract (balancing both, provider's and end-users' interests), which in my opinion, should be applicable to all European-based cloud providers.[207]

In order to draw this model, we will make reference to some of the findings already mentioned in the second chapter, and assess whether some clauses of the most established contracts in USA would be suitable in the European framework.

Note that the contract we will draft should be understood as a basic level of protection, which could be additionally implemented via negotiation in specific cases.

4.1 Data Protection

4.1.1.Data controller and Data Processor

As already stated in the second chapter, it urges to set a detailed list when a provider should be considered either controller or processor, in the cloud computing scenario. Once these definitions are clear, there will not be confusion about who needs to secure the data kept and processed in a cloud-computing relationship. A practical way to find out who should be understood as controller could be by answering some simple questions[208] in a case by case processing scenario:

-Is the provider an expert in its field?

-Which decisions are taken by the provider over the processing?

-Does the end-user understands that the services contracted are performed through a cloud provider?

[207] Remember that the DPD might be applicable to non-European cloud providers which do not even have an establishment within a Member State (article 4.1 c). Contrary, the eCommerce Directive regulating to "non-personal data" applies to information society services established within Member States territory. Therefore, since their scope of applicability of both Directives is not the same, not all the cloud providers needing to apply the DPD would equally need to apply the eCommerce Directive, and the opposite. This might be the case of a non-European cloud provider not having any establishment within Member States, but using equipment situated within this territory for the processing of personal data.

That is why we propose the model contract to be mandatory only for European-based cloud providers, which clearly fall within the applicability of both Directives.

[208] These questions where already pointed out by Gilbert F. See Supra n80,14-15.

Answering these questions we could find out the involvement of the provider in the processing of data, and its possible categorization as controller when from the questions it seems obvious that the provider is acting independently.[209]

We need to remember that, cloud providers can be both processors and controllers for different parts of the processing operation. Therefore, the security measures proposed to secure such data could be carried out by one party to other, depending on the purpose of the personal data processed.

4.1.2 Security measures

In the second chapter we pointed out that the security measures established by the DPD are implemented differently across Europe. Hence, European end-users are confronted with different levels of protection.

In our opinion, the "*appropriate technical and organizational measures to protect data"*[210] should be detailed and in compliance with an external standard, for instance, the ISO/IEC 27001. The goal of the just cited standard is to "*provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an Information Security Management System*".[211] Through this security standard, organizations security processes would be analyzed and tested against the requirements set in the standard. Therefore, an independent auditor guarantees that the organization meets the security controls and activities set by ISO. Companies would deliver the audit certification to the end-user of the service that would be aware of the security controls carried out by the provider.

Therefore, when the cloud-provider is understood "processor", the following clause applies[212]:

> "*We*[213] *will take strict measures to ensure that the customer's data is treated securely and protected against unauthorized or unlawful processing, accidental loss, damage or destruction. Hence, We shall encrypt Your personal data before keeping or transfer it to other parties. Moreover, our centers are protected against third parties unlawful*

[209] Ibid,15.

[210] Article 17 DPD (See Supra 65).

[211] Cited extracted from the "ISO 27000 Directory", < http://www.27000.org/iso-27001.htm>. Accessed 24th March 2012. For further information about this standard, visit <http://www.27000.org/index.htm>.

[212] Remember that European-based cloud providers offering "electronic communication services" are affected by both, the "cookie Directive", which in its article 4.1 establishes some additional security measures when processing personal data and the article 7 of the DRD, setting additional security measures over the data retained (apart from those displayed in the DPD) for providers.

[213] Hereinafter WE refers to the cloud provider.

access by physical security measures such as passwords codes. Any access to Your data Shall be logged in order to determine whether it is lawful or not. Such measures will be carried out in accordance with the security management information granted by the ISO/IEC 27000. All information regarding these measures and the certification process will be available to You[214] upon request.[215]

The same clause should apply when the cloud-provider is considered "controller", however, in this second scenario additional measures apply:

"*We ensure that Your data will be treated qualitatively in accordance with the DPD*[216]*. Moreover, We shall provide You with the purposes of the processing and any further information You may require Us. You shall execute Your right to access the data We are processing at any time over the term of This Agreement".*

4.1.3 Geographical location of data and transfer

Due to the nature of clouds, personal data can be transferred among different jurisdictions depending on which server offers capacity and availability[217]. Under the current framework this fact can affect negatively end-users since not all of them will have their data subjected to the same law and security measures.

In our proposed contract, we will follow the text of the DPD when it says that cloud providers are not allowed to transfer end-users' personal data outside the EEA to third countries, which do not present an adequate level of protection (unless the end-user gives its consent). However, we suggest adapting a similar clause to the one displayed by Amazon[218], offering end-users the possibility to choose the region where they want their data to be stored, transferred to and processed.

This "choice of region" is irrelevant from the DPD perspective as long as the content remains within the EEA, however, end-users may have a special interest in keeping their data in a certain region due to the different security measures which different regions may present when

[214] Hereinafter YOU refers to the end-user.

[215] Note that in the case the Cookie Directive would be applicable, the ISO certification should also guarantee that the security measures established in its article 4 are taken. Additionally, the security measures settled in the article 7 of the DRD should equally be guaranteed.

[216] Article 6 DPD.(See Supra n65).

[217] Graham R. and Bahra J. "Cloud Computing in the European Union" Edwards Wildman (2012),2 <http://www.edwardswildman.com/files/News/0dde5c04-2da5-470a-ae0c-fca84e68bb40/Presentation/NewsAttachment/7795fe40-8b0c-4f2d-9c86-fd8a5b7eb7ae/CloudComputingEuropeanUnion.pdf>. Accessed 24yh April 2012.

[218] AWS Amazon Customer Agreement, clause 3.2 (See Supra n13).

processing personal data[219], or due to the mere distance from the end-users' location. Thus, the closest the data is processed or stored, the quickest it may be accessed by the end-user.

> *"You may specify the European regions in which Your Content will be stored and accessible by You and transferred among. Thereinafter We will only move Your Content from your selected region/s after notifying you and having your consent unless We are obliged to comply with the law or request made by law enforcement, regulatory agencies or civil actions"*

4.2 Intellectual Property Rights

Following the most extended trend in both USA and Europe, we would suggest not to grant any IP right (license) to the other contracting party.

Hence, we will avoid problems concerning the position of controller that the cloud-provider might have over the end-users content.[220] In such way end-users have a higher control over their content, being the only ones deciding upon its use and purpose.

As already said, this scenario seems to be the most extended one. However, while all the contracts analyzed mention that the provider will not transfer any right to the end-user, not all of them provide the right of the end-user to preserve their IP rights.[221]

Therefore, the proposed clause will clearly express that both parties preserve their respective IP rights.

> "*No contracting party will transfer to the other, any ownership right, title or license over its content or data, including any intellectual property right".*

4.3 Confidentiality and Disclosure

4.3.1 Confidential information

Although all the providers seem to agree upon the scope of its meaning, we advise to determine which data should and which one should not be treated confidentially.

[219]Note that some providers can implement the present contract with higher security measures than the ones displayed here.

[220] See Supra n107.

[221] Just Salesforce and Amazon do it. (See Supra n104.)

"*Either party shall not disclose the other's contracting party data or information revealing any aspect or its businesses, no matter whether its knowledge comes in written or verbal format. Information should be considered as confidential when it is not available to the public. Therefore, already known information by the receiving party should not be understood as confidential information".*

4.3.2 Security

As we already explained in the second chapter, confidential information fits under the definition of personal data, thus, the DPD security measures explained above for the processing of personal data, are also applicable to confidential information.

Additionally, the contract should make clear reference to the mutual obligation to treat the data confidentially[222]. However, we consider that the expected security measures to take by both parties should be detailed in the agreement.

"*Either party shall keep the other's contract party data confidentially. This obligation also involves both parties' staff, affiliates' staff or subcontractors, who shall sign a confidentiality agreement before accessing and processing the data. This mutual duty lasts for one year once this Agreement is terminated, before accessing the data".*

4.3.3 Disclosure

We would restrict to objective situations, such as requests made by law, agencies or civil actions, the cases when such content may be disclosed. Moreover, we think that cloud-providers should be allowed to report authorities any end-user conduct which in their opinion might be contrary to Law. However, in this second case, providers must support this conduct by justified arguments. In every case, the previous notice to the other party should be required.

"We shall display Your information, previous notice to You, in response of any request made by law enforcement, regulatory agencies or civil actions. Additionally, we may report and support any conduct carried by You to the authorities as long as We consider that such behavior might be contrary to law."

4.4 Warranties and Disclaimers

[222] Article 16 DPD. (See Supra n65).

With regard to warranties, we suggest following the practice of European-based providers which warrantees the performance of the service as specified in theirs SLAs.[223] Additionally, we find interesting the clause of Cloudee which offers end-user different options to be taken when the service runs defectively or faultily. We propose to adopt as standard clause, the following one:

> "1. *We warrant that the service will be performed in conformance to the specifications detailed in the SLA[224]. If the service does not run in accordance to these specifications, You shall notify us the failure. Thereby You can decide whether you would like us to return the fees paid by you since the service did not run properly, repair or terminate the service. Any of the just mentioned solutions will be free of charge.*
> *2. We are not responsible for any failure or delay resulting from the communication network in any case".*

To make clear the responsibility of the cloud-provider, we would suggest introduce clear disclaimer, which would say as follows:

> *"3. Any additional warranty not included in this agreement is excluded."*

4.5 Limitation of Liability

With regard to direct damages, we would propose to follow the European strategy and describe the cases under which the cloud provider is liable[225]. The clause drafted bellow will address to the most common circumstances which mostly all the contracts analyzed seem to agree upon.

> *"1. We will only be liable (including any act performed by Our employees or third parties sub-contractors) to You in respect of:*
> *a. breach of the Contract (including unlawful disclosure of data or breach of security measures when processing, storing and transferring your data or content);*
> *b. normal use of the service made by You;*

[223] We will not enter to standardize how SLAs should specify the performance of the service, since not all the services offered by cloud-providers present the same features, so their performance cannot be warranted equally.

[224] Usually SLAs make mention to the following topics, which may vary from one provider to other (depending on the service offered): Support, response times, accessibility, performance, exclusions and other services. Third-parties monitoring should also be included (See Supra n35).

[225] The American trend of excluding the cloud-providers' liability for direct damages to the extent permitted by Law, does not seem transparent, since the law applicable to the relationship between provider and end-users, may differ and these latters may not be aware of the limits set by the applicable law.

c. additional service provided by us necessary for the normal performance of the webservice contracted; and
d. any mistake or misleading act coming from Our company and negatively affecting this Agreement or the service contracted.

The liability arising under such paragraph will be restricted to the higher quantity between a fixed amount (still need to be fixed by the competent authority) and the amount paid by You over the last twelve months before the incidence took place.

2. Our liability will never be excluded in cases:
a. of death or personal injury caused by our negligence; or
b. of fraudulent performances by Us; or

In these two cases, the monetary restriction expressed in the paragraph 1 will not take place.[226]*"*

Referring to indirect damages, we also advise to name the circumstances under which the cloud-provider is not liable, which in most analyzed contracts relates to the following:

"3.We will not be held liable for any losses or damages suffered by You, when those damages are arising in contract, tort or otherwise and fall within any of the following categories:
a. Loss of profits;
b. Loss of business opportunity;
c. Loss of goodwill;
d. Loss of data as long as we perform the security measures in accordance with the ISO27000.

To finish with, we would like to talk about the "force majeure" clause. Such clause is already included in almost all the contracts analyzed, but just Twinfield offers the possibility of termination of the contract in case the delaying event takes more than 60 days and after written notice to the other party. Therefore, we suggest to follow a similar standard clause:

"*The company is not liable for any failure or latency in the performance of its duties arising from this Agreement, when these failures are caused by a force majeure element*[227] *.If any delaying event under the paragraph above lasts for a period of at*

[226] Such exclusion of monetary limitation is just found in the contract offered by Microsoft. (See Supra n129).

[227] Force majeure includes a failure of the company's supplier, measures taken by the Government, power, internet or telephone cuts and any other case outside the cloud providers' control.

least 60 days, either Party may terminate this Agreement in 14 days by giving previous written notice to the other party."

4.6 Indemnifications

4.6.1 Indemnification by the end-User

As already mentioned in the second chapter, cloud providers refer to this topic differently, since some of them add more causes which trigger the end-user obligation to indemnify their cloud-provider. However, since the aim of this third chapter is to create a standard contract, we suggest setting as standard, just those clauses that mostly all providers seem to agree upon. Additionally, due to the same reason, we propose introducing the previous notice mechanism. To end with, we find the reservation right held by Cloudee to control the defense, a very good idea, because otherwise, the provider should be held liable without being given the opportunity of defending himself.

> *"You shall defend Us against any claim made by a third party claiming an infringement in its intellectual property caused by Your content*[228]*, or Your use of the Services breaching this Agreement or applicable law. In any of these cases, You must indemnify Us for any damages, attorney fees and costs finally conferred against Us; provided that We give You written notice of the claim against Us. Additionally, We reserve the right, at Your own expenses, to assume the exclusive defense and control of any matter subject to indemnification by You."* [229]

4.6.2 Indemnification by the cloud provider

As we have already seen in the second chapter, just some US-based providers include this clause in their agreements. In order to protect end-users, we find necessary to include such clause in a standard contract.

To find a balance between both contracting parties, we think that the cited clause should be written in the same way as the paragraph above. Therefore we advise to broaden the

[228] This content cannot be personal data.

[229] Adapted clause of Salesforce Master Subscription Agreement, clause 10.1 (See Supra n11).

subject matter of the indemnification further than just damages to third parties intellectual property by the use of the product itself.

> *"We shall defend You against any claim made by a third party claiming an infringement in a third party intellectual property, caused by Your normal use of the service We offer. In this case We must indemnify You for any damages, attorney fees and costs finally conferred against You; provided that You give Us written notice of the claim against You. Additionally, You may reserve the right, at Our own expenses, to assume the exclusive defense and control of any matter subject to indemnification by Us.*
>
> *We may, at Our own choice, modify the Service, obtain the needed license with the aim of continuing the use of the service, or terminate this Agreement."*

4.7 Law and Jurisdiction

Despite the requirements imposed by the Rome I and II Regulations in the EU scenario, contracting parties have freedom of choice to determine which law they want to apply to their contractual obligations. This allows both, cloud providers and customers to understand the jurisdiction chosen in anticipation.

Following the example displayed by Salesforce, we would propose to give to the end-user the choice between applying the provider's national law where he is based in or the law of the end-user domicile. Thus, not all the contracts held by the cloud provider would be governed by the same Law.

Actually this is already possible in practice when end-users are consumers (usually in IaaS and SaaS) because "*European consumers enjoy the right to always take action against a business in their home Jurisdiction. This undermines choices made by the provider in the contract"*[230]. However, we propose to clearly express this in the contract.[231]

---

[230] *See Svantesson D. and Roger Clarke R. "Privacy and consumer risks in cloud computing"* Bond University, Faculty of Law. (2010),13. <http://epublications.bond.edu.au/cgi/viewcontent.cgi?article=1346&context=law_pubs&sei-redir=1&referer=http%3A%2F%2Fwww.google.com%2Furl%3Fsa%3Dt%26rct%3Dj%26q%3Dprivacy%2520and%2520consumer%2520risks%2520in%2520cloud%2520computing%26source%3Dweb%26cd%3D1%26sqi%3D2%26ved%3D0CCsQFjAA%26url%3Dhttp%253A%252F%252Fepublications.bond.edu.au%252Fcgi%252Fviewcontent.cgi%253Farticle%253D1346%2526context%253Dlaw_pubs%26ei%3DBYqUT6v3OpKE8gOH3fzODA%26usg%3DAFQjCNHmp3ss8xvKhKJShQSyoXxziPX-Uw#search=%22privacy%20consumer%20risks%20cloud%20computing%22>. Accessed 23rd April 2012.

[231] We would propose such choice for every end-user, not just consumers. Therefore such clause would be applicable for every kind a service (SaaS, IaaS and PaaS). Note that in the CloudControl PaaS T&C (See Supra n16, clause 16.3) we see "*CloudControl is also entitled to sue at the user's place of performance*", but nothing is said about end-users right.

"This *Agreement and any dispute or claim arising from its subject should be governed by the laws of either, the country where You are domiciled or performing the service or the country where We are based in*[232]*. The applicable Law remains at Your choice".*

Following the example of Cloudee, the Courts which will need to have knowledge of the conflict are those of the country, which national law is applicable to the disputes. However, we should understand such jurisdiction as non-exclusive, leaving therefore the possibility to agree upon different courts by both parties.

"*This agreement and any subject rising from it should be submitted to the non-exclusive jurisdiction of the courts whose Law is applicable".*

4.8 Termination

4.8.1 Term

"*From the date You click into this agreement You accept all the conditions established into it which will last until the Service agreed upon expires or either party terminates it.*"

4.8.2 Ways of termination

As we said above, the proposed contract needs to balance the interests of both parties, therefore the termination for convenience should be available for both of them, and the termination for cause should gather the most common causes seen all over the contracts. Like this, contractual parties can know in advance the causes of termination of the contract.

In no case the service could be terminated without notice to the other party. Moreover, as Salesforce does, the contract should make mention to the refunds or payments needed to be done to the other party once the termination cause takes place.

"*Either party may terminate this agreement for convenience after giving a 30 days previous written notice to the other party.*

Either party may terminate this agreement for cause:

[232] There is a lot of discussion about where this is. We think that a cloud-provider should be considered based-in in the country where the core of its activities is carried out. This location does not necessary need to coincide with the one where the headquarters are.

(i) After giving a 30 days previous notice to the other party if this later breaches the agreement,

(ii) if the other party enters into an economic situation involving risk of in payment or performance of the service agreed upon, or

(iii) After giving a 14 days previous notice to the other party if a force majeure element lasts more than 60 days.

We may terminate this Agreement immediately after giving you 14 days previous written notice:

(i) if our relationship with a third party, providing Us essential services, expires, terminates or forces us to change the way we provide Our Service or,

(ii) to comply with law or any governmental entities' request.[233]

In case You exercise the termination for cause, We shall refund You any anticipated fee You might have done, covering the remaining term from the termination date. In case We exercise the termination for cause, You shall pay any due fee until the end of the term, from the termination date."[234]

4.8.3 Effects

Apart from the general effect of expiration of any right given, this part should solve how the data can be recovered. We consider the option given by Salesforce the best one, since after the end-user decides whether he wants to extract his data; this will be automatically deleted (without extra-fee).

"Once this Agreement terminates (either for cause or convenience), and upon previous 30 days written notice by You, We shall make available to You a downloadable file, in (.csv)[235] *format, displaying all the data we gathered about You over the term. After such 30-days period, we have no obligation to maintain or provide any of Your Data and shall therefore delete it, unless legally prohibited."*

[233] Adapted copy of the clause 7.2 (ii) of AmazonWeb Services Customer Agreement (See Supra n13). All the causes under this paragraph should be objective, not based on the provider's belief.

[234] Ibid Clause 12.5

[235] Format described in Salesforce Master subscription agreement, clause 12.5 (See Supra n11)

Remember that trough the article 15 of the eCommerce, cloud providers offering storage services might be required to retain certain end-user's data (IP addresses). [236]

4.9 Monitoring by Provider[237]

We do not think that the trend followed by US-based providers is the correct one, since from the moment they monitor end-users for commercial and promotion purposes; they automatically become controllers of the data they collect (in case the data is not anonymized first). This situation would be difficult in the relationship between the contracting parties, because the end-user would not be the one who decides over the purpose of this own data.

Therefore, we propose to establish as standard a clause where providers are just allowed to monitor end-users for statistical purposes. However, providers shall be required to previously anonymize the data collected.

> *"By entering in this agreement You allow us to use Your anonymized data just for statistical purposes".*

4.10 Exit

Finally, we strongly recommend to mention the end-user right to data portability, in order not to affect competition Law. It is necessary to allow end-users to simply access their data and programs for running them in other sites or just withdraw them from the cloud. Otherwise end-users could find themselves locked-in[238]. Just like this the cloud environment could be described as competitive and open.

---

[236] As we already mentioned in the third Chapter, cloud providers offering electronic communication services, should retain the data not less than six months and not more than two years from the date of the communication, in accordance with the article 6 of the DRD.

[237] Remember that such monitoring can take place though the use of cookies. Through the Cookie Directive ECS cloud providers would need to ask end-users for previous consent in order to get any information from them through the use of cookies.

[238] As we have already mentioned in the second chapter, the limitation of data portability could fit under an act prohibited by competition Law. This just cited distortion of competition Law can be reached in different ways, according to the service contracted. In IaaS, providers should allow end-users to run the applications under their IaaS into another IaaS service provider. When talking about PaaS, any application developed in the platform, should be portable to other providers' platforms. In SaaS, they should be able to be run in different networks. (See Supra n22, pages 3, 4, 24 and 25).

It is important to mention that none of the contracts analyzed make mention of this issue. Although it does not mean that data or content run in their servers cannot be portable to others cloud providers'.

> *"You shall at any time revers, port and access your data or content to be run in other providers' services".*

CONCLUSION AND RECOMMENDATIONS

As already cited throughout the thesis, understanding of cloud providers as ECSs, would mean the applicability of the ePrivacy Directive and the Data Retention Directive to the cloud services. This scenario would present higher and stricter obligations than the ones already proposed.[239]

The main problem is that it is still not clear whether cloud computing providers should be equal to ECSs due to the nature of the different cloud services. Although it is true that some cloud services could fit within the wording of ECS, because their nature focuses on the transmission of the service (this might be the case of some SaaS), others show a different nature focusing on the content of the service they offer .Therefore, we do not think that it would be advisable to generalize the applicability of the Cookie Directive and the Data Retention Directive to cloud computing services since they greatly differ ones from others.

That is why the standard contract was not implemented with these two directives. Their applicability would be desirable if all the cloud computing services fit within the nature of ECSs. Therefore, it is the nature of the service which determines whether those directives are applicable or not to the contract.

Recommendation one:
To bring legal certainty into cloud computing services, it would be viable to better clarify the meaning of "electronic communication services", and individually identify which cloud services fall within its scope.

To sum up, we would like to summarize which US-based clauses could be adapted within the European context. Hence the research question displayed in the introduction will be answered.

Firstly, we consider the Amazon's clause[240] relating to Geographical location of data and transfer very interesting and favorable to end-users. Just like this end-users would have complete knowledge regarding where their data is located. Moreover, if the end-user chooses a close region, the service might be optimized by a higher speed of performance and even a minimization of the cost.

[239] DPD and eCommerce Directives.

[240] AWS Amazon Customer Agreement, clause 3.2 (See Supra n13).

Recommendation two:
Grant end-users the option to choose a region (within the EEA) where their data is going to be stored, transferred and processed.

In second place, we suggest to follow the example of US-based providers, since none of them establish the granting of licenses over end-user IP rights to the provider. As we already explained, it does not seem reasonable to force end-users to grant licenses over their content, since they are those who should, at their own discretion, dispose with their rights. Moreover, this situation would finish with end-user concerns regarding the controller's position that providers would held over the licensed IP content.

Recommendation three:
Set a clause which expresses the right for both parties not to grant any Intellectual Property Rights or license over each ones' Intellectual Property content to the other contracting party.

In the second chapter we already saw that personal information needs to be processed confidentially by both provider and end-user (including their staff). Therefore, we would recommend making clear the scope of "confidential information" explaining which information fits, and which one does not fit within its scope. This detailed way to define the meaning of confidentiality and its application, was introduced by Salesforce.[241]

Recommendation four:
Set a definition which explains what is and what is not understood as confidential information. Moreover, all the measures to be taken should be explained and added into the contract.

Additionally, when talking about law and jurisprudence, we find the option taken by Salesforce[242] the most suitable one, because end-users are given the possibility to bring any claim to the jurisdiction which suits them the most.

[241] Salesforce Master Subscription Agreement, clause 8.1 (See Supra n11).

[242] Ibid, clause 13.

Recommendation five:

Each end-user shall have the option to bring any dispute arising during the term of the service either to the jurisdiction where the provider is based in[243] or the one of end-user domicile (or a place of performance in case the end-user is a business).

We would like to point out that the standard contract suggested in the fourth chapter should be understood as a minimum level of protection[244] for every European end-user. Therefore, cloud-providers can raise the level of protection offered by this standard contract.

All these recommendations explained above, make mention to US clauses which we think display interesting points to be introduced into the European legal framework. The proposed contract answers current needs presented in the Cloud Computing scenario, and therefore it could fit under the "new strategy" for cloud computing promoted by the European Commission. Actually, the implementation of this contract would suppose a further step towards the developing of the "Digital Single Market"[245] composing the first pillar of the Digital Agenda for Europa.

Finally, we would like to propose the setting of an international standard contract model, because we cannot forget that the cloud services operate over a network (internet) which has no boundaries, and all end-users' should be protected at the same level regardless to the place where their data is actually processed. Hence standardization should look for global standards enabling, among other requirements, interoperability and data portability among Clouds-providers offering the same level of protection for end-users.

[243] See Supra n232.

[244] Note that apart from the contract explained in the third chapter, cloud providers offering electronic communication services should additionally implement the Cookie Directive and the DRD.

[245] For further information check the following link <http://ec.europa.eu/information_society/newsroom/cf/pillar.cfm>. Accesses 9th June 2012.

BIBLIOGRAPHY:

Articles and Journals

A. H. Schmidt "Cloud computing legal framework and privacy" (2011) Hacking,32-40.

Buono L. "The Global Challenge of Cloud Computing and EU Law", (2010), The European Criminal Law Association's Forum.

Da Correggio Luciano L. and Walden I. " Ensuring competition in the Clouds: The role of competition Law?" (2011) Social Science Research Network.

Gilber F "Cloud Service Providers as Joint-Data Controller" (2011) IT Law Group.

Graham R. and Bahra J. "Cloud Computing in the European Union" Edwards Wildman (2012).

JISC Legal Information "User Guide : Cloud Computing Contracts, SLAs and Terms & Conditions of Use" (2011).

Joint A. and Baker E. "Knowing the past to understand the present- issues in the contracting for cloud based services"(2011), computer law & security review 27 , 408-410 .

Leenes R. "Who Controls the Cloud?" (2010), Revista de Internet, Derecho y Política.

McKendrick J. "US Lags Much of World in Cloud Computing Adoption: Study" (2012) Forbes.

Moiny, J.P. "Are Internet protocol addresses personal data? The fight against online copyright infringement" (2011), computer law & security review.

Patel P., Ranabahu A.and Sheth A. "Service Level Agreement in Cloud Computing" (2009), Knoesis Center, Wright State University, USA and DA-IICT, Gandhinagar, INDIA.

S. Subashini and V. Kavitha "A survey on security issues in service delivery models of cloud computing" (2010) Journal of Network and Computer Applications.

Stratford J.S. & Stratford J. "Data Protection and Privacy in the United States and Europe", (1998) Yale University.

Vincent M. and Hart N., "Legal issues in the Cloud - Part 3" (2011) CIO. <http://www.cio.com.au/article/382652/legal_issues_cloud_-_part_3/>.

Vincent M. and Hart N., “Legal issues in the Cloud - Part 4” (2011) CIO. <http://www.cio.com.au/article/382657/legal_issues_cloud_-_part_4/>.

Blogs

Cloud Tweaks plugging into the cloud “Top 25 European Cloud Computing Rising Stars To Watch – Complete List.” (2011). <http://www.cloudtweaks.com/2011/04/top-25-european-cloud-computing-rising-stars-to-watch-complete-list/>.

Hon K. “Who's responsible for personal data in cloud computing? You and your Saas, Paas and IaaS providers”, (2011)COMPUTERWORLDUK, CloudVision

Interview

Balboni P. "Data Protection and cloud computing: the need for global standards” (2011) Youtube .

Legislation

Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts *OJ L 095, 21/04/1993.*

Directive 2000/31/EC of The European Parliament and of The Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce) OJ L 178/1, 17.7.2000.

Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services, OJ L 108/33 24.4.2002.

Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector. of the European Parliament and of the Council of 12 July 2002 (Directive on privacy and electronic communications), OJ L 201/37 31.7.2002.

Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ L 105, 13.4.2006.

Directive 2009/136/EC of The European Parliament and of The Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users’ rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and

Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws.

Directive 2009/140/EC OF The European Parliament and of The Council of 25 November 2009, amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorization of electronic communications networks and services, OJ L 337/37, 18.12.2009.

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data on the free movement of such data, *OJ L 281 , 23/11/1995.*

Federal Data Protection Act (BDSG), December 20, 1990 (BGBl.I 1990 S.2954), as amended by the law of 14 September, 1994 (BGBl. I S. 2325).

Federal Act on Data Protection of 19 June 1992,235.1, the Federal Assembly of the Swiss Confederation.

Master Thesis

Pavel B. V. "Cloud Computing and The Regulatory Framework for Telecommunications and Information Society Services" (2012) Tilburg University.

Official documents, opinions and Speeches.

"ARTICLE 29 Data Protection Working Party" WP 113 (2005).

"Survey by IEEE and Cloud Security Alliance details importance and urgency of Cloud Computing Security Standards" (2010) IEEE Standards Association. <http://standards.ieee.org/news/2010/cloudcomp.html>.

Buono L. "The Global Challenge of Cloud Computing and EU Law", (2010), The European Criminal Law Association's Forum.

Commission of the European Communities, Information Society & Media Directorate-General, Software & Service Architectures, Infrastructures and Engineering Unit. Cloud Computing Hearing with Users: Meeting Note" (2011), 4. Europe's information society, thematic portal.

"Hearing with Telecommunication and Web Hosting Industry ",Commission of the European Communities, Information Society & Media Directorate-General, Software & Service Architectures, Infrastructures and Engineering Unit (2011).

Hogan M., Liu f. and Sokol A. "NIST Cloud Computing Standards Roadmap" (2011), National Institute of Standards and Technology , special Publication 500-291.

Hustinx P. "Data Protection and Cloud Computing under EU law"(2010) European Data Protection Supervisor.

IP/11/575 "Digital Agenda: Commission seeks views on how best to exploit cloud computing in Europe" Europa press releases (2011).

Kroes N. SPEECH/12/38 "Setting up the European Cloud Partnership World Economic Forum Davos, Switzerland, 26th January 2012" Europa press releases (2012).

Mell P. and Grance T. "The NIST Definition of Cloud Computing" (2011). NIST National Institute of Standards and Technology.

Opinion 1/2010 on the concepts of "controller" and "processor", 00264/10/EN, WP 169 (2010).

Opinion 5/2009 on Online Social Network; 01189/09/EN, WP 163, (2009).

Opinion 4/2007 on the concept of personal data , 01248/07/EN WP 136, (2007).

Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites, 5035/01/EN/Final, WP 56(2002).

Websites

Amazon.com

CloudControl.com

Cloudee.eu

CloudSigma.com

Ec.europa.eu

Salesforce.com

The ISO 27000 Directory <http://www.27000.org/>, <http://www.27000.org/iso-27001.htm>.

Twinfield.nl, which remits to the English website: Twinfield.co.uk

Windowsazure.com

Working papers

Bradshaw S., Millard C. and Walden I. "Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services" (2010) Queen Mary University of London, School of Law. Legal Studies Research Paper No.63/2010 .

Hon K., Hörnle J. and Millard C. " Data Protection Jurisdiction and Cloud Computing – When are Cloud Users and Providers Subject to EU Data Protection Law? The Cloud of Unknowing, Part 3"(2011) Queen Mary University of London, School of Law Legal Studies Research Paper No 84/2011.

Hon W. K., Millard C. and Walden I "The Problem of 'Personal Data' in Cloud Computing - What "Information is Regulated? The Cloud of Unknowing, Part 1", (2011) Queen Mary School of Law Legal Studies Research Paper No. 75/2011.

Hon W. K., Millard C. and Walden I. " Who is responsible for personal data in cloud computing? The cloud of unknowing, Part 2", (2011) *Queen Mary School of Law Legal Studies Research Paper No. 77/2011*.

Industry Recommendations to Vice President Neelie Kroes on the orientation of a European Cloud Computing Strategy (2011).

Jasper P. Sluijs, Pierre Larouche and Wolf Sauter "Cloud Computing in the EU Policy Sphere" Tilburg University. TILEC Discussion Paper DP 2011-036 (2011).

Marston S.., Li Z., Bandyopadhyay S. and Zhang J. "Cloud Computing – The Business Perspective" (2009) University of Florida.-Warrington College of Business Administration.

Svantesson D. and Roger Clarke R. "Privacy and consumer risks in cloud computing" Bond University, Faculty of Law. (2010).

ANNXES

Annex 1: SALESFORCE MASTER SUBSCRIPTION AGREEMENT

THIS MASTER SUBSCRIPTION AGREEMENT (“AGREEMENT”) GOVERNS YOUR ACQUISITION AND USE OF OUR SERVICES.

IF YOU REGISTER FOR A FREE TRIAL FOR OUR SERVICES, THIS AGREEMENT WILL ALSO GOVERN THAT FREE TRIAL.

BY ACCEPTING THIS AGREEMENT, EITHER BY CLICKING A BOX INDICATING YOUR ACCEPTANCE OR BY EXECUTING AN ORDER FORM THAT REFERENCES THIS AGREEMENT, YOU AGREE TO THE TERMS OF THIS AGREEMENT. IF YOU ARE ENTERING INTO THIS AGREEMENT ON BEHALF OF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY AND ITS AFFILIATES TO THESE TERMS AND CONDITIONS, IN WHICH CASE THE TERMS "YOU" OR "YOUR" SHALL REFER TO SUCH ENTITY AND ITS AFFILIATES. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT AGREE WITH THESE TERMS AND CONDITIONS, YOU MUST NOT ACCEPT THIS AGREEMENT AND MAY NOT USE THE SERVICES.

You may not access the Services if You are Our direct competitor, except with Our prior written consent. In addition, You may not access the Services for purposes of monitoring their availability, performance or functionality, or for any other benchmarking or competitive purposes.

This Agreement was last updated on September 15, 2011. It is effective between You and Us as of the date of You accepting this Agreement.

Table of Contents

8. Confidentiality

9. Warranties and Disclaimers

10. Mutual Indemnification

11. Limitation of Liability

12. Term and Termination

13. Who You Are Contracting With, Notices, Governing Law and Jurisdiction

14. General Provisions

1. DEFINITIONS

"Affiliate" means any entity which directly or indirectly controls, is controlled by, or is under common control with the subject entity. "Control," for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

"AppExchange" means the online directory of applications that interoperate with the Services, located at http://www.salesforce.com/appexchange or at any successor websites.

"Malicious Code" means viruses, worms, time bombs, Trojan horses and other harmful or malicious code, files, scripts, agents or programs.

"Non-Salesforce.com Applications" means online applications and offline software products that are provided by entities or individuals other than Us and are clearly identified as such, and that interoperate with the Services,

including but not limited to those listed on the AppExchange and those identified as Force.com Labs or by a similar designation.

"Order Form" means the documents for placing orders hereunder, including addenda thereto, that are entered into between You and Us or any of Our Affiliates from time to time, including addenda and supplements thereto. By entering into an Order Form hereunder, an Affiliate agrees to be bound by the terms of this Agreement as if it were an original party hereto. Order Forms shall be deemed incorporated herein by reference.

"Purchased Services" means Services that You or Your Affiliates purchase under an Order Form, as distinguished from those provided pursuant to a free trial.

"Services" means the products and services that are ordered by You under a free trial or an Order Form and made available by Us online via the customer login link at http://www.salesforce.com and/or other web pages designated by Us, including associated

offline components, as described in the User Guide. "Services" exclude Non-Salesforce.com Applications.

"User Guide" means the online user guide for the Services, accessible via login at http://www.salesforce.com, as updated from time to time. You acknowledge that You have had the opportunity to review the User Guide during the free trial described in Section 2 (30-Day Free Trial) below.

"Users" means individuals who are authorized by You to use the Services, for whom subscriptions to a Service have been ordered, and who have been supplied user identifications and passwords by You (or by Us at Your request). Users may include but are not limited to Your employees, consultants, contractors and agents, and third parties with which You transact business.

"We," "Us" or "Our" means the salesforce.com company described in Section 13 (Who You Are Contracting With, Notices, Governing Law and Jurisdiction).

"You" or "Your" means the company or other legal entity for which you are accepting this Agreement, and Affiliates of that company or entity.

"Your Data" means all electronic data or information submitted by You to the Purchased Services.

2. FREE TRIAL

If You register on our website for a free trial, We will make one or more Services available to You on a trial basis free of charge until the earlier of (a) the end of the free trial period for which you registered or are registering to use the applicable Service or (b) the start date of any Purchased Services ordered by You. Additional trial terms and conditions may appear on the trial registration web page. Any such additional terms and conditions are incorporated into this Agreement by reference and are legally binding.

ANY DATA YOU ENTER INTO THE SERVICES, AND ANY CUSTOMIZATIONS MADE TO THE SERVICES BY OR FOR YOU, DURING YOUR FREE TRIAL WILL BE PERMANENTLY LOST UNLESS YOU PURCHASE A SUBSCRIPTION TO THE SAME SERVICES AS THOSE COVERED BY THE TRIAL, PURCHASE UPGRADED SERVICES, OR EXPORT SUCH DATA, BEFORE THE END OF THE TRIAL PERIOD. YOU CANNOT TRANSFER DATA ENTERED OR CUSTOMIZATIONS MADE DURING THE FREE TRIAL TO A SERVICE THAT WOULD BE A DOWNGRADE FROM THAT COVERED BY THE TRIAL (E.G., FROM ENTERPRISE EDITION TO PROFESSIONAL EDITION OR FROM PROFESSIONAL EDITION TO GROUP EDITION); THEREFORE, IF YOU PURCHASE A SERVICE THAT WOULD BE A DOWNGRADE FROM THAT COVERED BY THE TRIAL, YOU MUST EXPORT YOUR DATA BEFORE THE END OF THE TRIAL PERIOD OR YOUR DATA WILL BE PERMANENTLY LOST.

NOTWITHSTANDING SECTION 9 (WARRANTIES AND DISCLAIMERS), DURING THE FREE TRIAL THE SERVICES ARE PROVIDED "AS-IS" WITHOUT ANY WARRANTY.

Please review the User Guide during the trial period so that You become familiar with the features and functions of the Services before You make Your purchase.

3. PURCHASED SERVICES

3.1. Provision of Purchased Services. We shall make the Purchased Services available to You pursuant to this Agreement and the relevant Order Forms during a subscription term. You agree that Your purchases hereunder are neither contingent on the delivery of any future functionality or features nor dependent on any oral or written public comments made by Us regarding future functionality or features.

3.2. User Subscriptions. Unless otherwise specified in the applicable Order Form, (i) Services are purchased as User subscriptions and may be accessed by no more than the specified number of Users, (ii) additional User subscriptions may be added during the applicable subscription term at the same pricing as that for the pre-existing subscriptions thereunder, prorated for the remainder of the subscription term in effect at the time the additional User subscriptions are added, and (iii) the added User subscriptions shall terminate on the same date as the pre-existing subscriptions. User subscriptions are for designated Users only and cannot be shared or used by more than one User but may be reassigned to new Users replacing former Users who no longer require ongoing use of the Services.

4. USE OF THE SERVICES

4.1. Our Responsibilities. We shall: (i) provide Our basic support for the Purchased Services to You at no additional charge, and/or upgraded support if purchased separately, (ii) use commercially reasonable efforts to make the Purchased Services available 24 hours a day, 7 days a week, except for: (a) planned downtime (of which We shall give at least 8 hours notice via the Purchased Services and which We shall schedule to the extent practicable during the weekend hours from 6:00 p.m. Friday to 3:00 a.m. Monday Pacific Time), or (b) any unavailability caused by circumstances beyond Our reasonable control, including without limitation, acts of God, acts of government, floods, fires, earthquakes, civil unrest, acts of terror, strikes or other labor problems (other than those involving Our employees), Internet service provider failures or delays, or denial of service attacks, and (iii) provide the Purchased Services only in accordance with applicable laws and government regulations.

4.2. Our Protection of Your Data. We shall maintain appropriate administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of Your Data. We shall not (a) modify Your Data, (b) disclose Your Data except as compelled by law in accordance with Section 8.3 (Compelled Disclosure) or as expressly permitted in writing by

You, or (c) access Your Data except to provide the Services and prevent or address service or technical problems, or at Your request in connection with customer support matters.

4.3. Your Responsibilities. You shall (i) be responsible for Users' compliance with this Agreement, (ii) be responsible for the accuracy, quality and legality of Your Data and of the means by which You acquired Your Data, (iii) use commercially reasonable efforts to prevent unauthorized access to or use of the Services, and notify Us promptly of any such unauthorized access or use, and (iv) use the Services only in accordance with the User Guide and applicable laws and government regulations. You shall not (a) make the Services available to anyone other than Users, (b) sell, resell, rent or lease the Services, (c) use the Services to store or transmit infringing, libelous, or otherwise unlawful or tortious material, or to store or transmit material in violation of third-party privacy rights, (d) use the Services to store or transmit Malicious Code, (e) interfere with or disrupt the integrity or performance of the Services or third-party data contained therein, or (f) attempt to gain unauthorized access to the Services or their related systems or networks.

4.3. Usage Limitations. Services may be subject to other limitations, such as, for example, limits on disk storage space, on the number of calls You are permitted to make against Our application programming interface, and, for Services that enable You to provide public websites, on the number of page views by visitors to those websites. Any such limitations are specified in the User Guide. The Services provide real-time information to enable You to monitor Your compliance with such limitations.

5. NON-SALESFORCE.COM PROVIDERS

5.1. Acquisition of Non-Salesforce.com Products and Services. We or third parties may from time to time make available to You (e.g., through the AppExchange) third-party products or services, including but not limited to NonSalesforce.com Applications and implementation, customization and other consulting services. Any acquisition by You of such non-salesforce.com products or services, and any exchange of data between You and any non-salesforce.com provider, is solely between You and the applicable non-salesforce.com provider. We do not warrant or support nonsalesforce.com products or services, whether or not they are designated by Us as "certified" or otherwise, except as specified in an Order Form. Subject to Section 5.3 (Integration with Non-Salesforce.com Services), no purchase of non-salesforce.com products or services is required to use the Services except a supported computing device, operating system, web browser and Internet connection.

5.2. Non-Salesforce.com Applications and Your Data. If You install or enable Non-Salesforce.com Applications for use with Services, You acknowledge that We may allow providers of those Non-Salesforce.com Applications to access Your Data as required for the interoperation of such Non-Salesforce.com Applications with the Services. We shall not be responsible for any disclosure, modification or deletion of Your Data resulting from any such access by NonSalesforce.com Application providers. The Services shall allow You to restrict

such access by restricting Users from installing or enabling such Non-Salesforce.com Applications for use with the Services.

5.3. Integration with Non-Salesforce.com Services. The Services may contain features designed to interoperate with Non-Salesforce.com Applications (e.g., Google, Facebook or Twitter applications). To use such features, You may be required to obtain access to such Non-Salesforce.com Applications from their providers. If the provider of any such Non-Salesforce.com Application ceases to make the NonSalesforce.com Application available for interoperation with the corresponding Service features on reasonable terms, We may cease providing such Service features without entitling You to any refund, credit, or other compensation.

6. FEES AND PAYMENT FOR PURCHASED SERVICES

6.1. Fees. You shall pay all fees specified in all Order Forms hereunder. Except as otherwise specified herein or in an Order Form, (i) fees are based on services purchased and not actual usage, (ii) payment obligations are non-cancelable and fees paid are non-refundable, and (iii) the number of User subscriptions purchased cannot be decreased during the relevant subscription term stated on the Order Form. User subscription fees are based on monthly periods that begin on the subscription start date and each monthly anniversary thereof; therefore, fees for User subscriptions added in the middle of a monthly period will be charged for that full monthly period and the monthly periods remaining in the subscription term.

6.2. Invoicing and Payment. You will provide Us with valid and updated credit card information, or with a valid purchase order or alternative document reasonably acceptable to Us. If You provide credit card information to Us, You authorize Us to charge such credit card for all Services listed in the Order Form for the initial subscription term and any renewal subscription term(s) as set forth in Section 12.2 (Term of Purchased User Subscriptions). Such charges shall be made in advance, either annually or in accordance with any different billing frequency stated in the applicable Order Form. If the Order Form specifies that payment will be by a method other than a credit card, We will invoice You in advance and otherwise in accordance with the relevant Order Form. Unless otherwise stated in the Order Form, invoiced charges are due net 30 days from the invoice date. You are responsible for providing complete and accurate billing and contact information to Us and notifying Us of any changes to such information.

6.3. Overdue Charges. If any charges are not received from You by the due date, then at Our discretion, (a) such charges may accrue late interest at the rate of 1.5% of the outstanding balance per month, or the maximum rate permitted by law, whichever is lower, from the date such payment was due until the date paid, and/or (b) We may condition future subscription renewals and Order Forms on payment terms shorter than those specified in Section 6.2 (Invoicing and Payment).

6.4. Suspension of Service and Acceleration. If any amount owing by You under this or any other agreement for Our services is 30 or more days overdue (or 10 or more days overdue in the case of amounts You have authorized Us to charge to Your credit card), We may, without limiting Our other rights and remedies, accelerate Your unpaid fee obligations under such agreements so that all such obligations become immediately due and payable, and suspend Our services to You until such amounts are paid in full. We will give You at least 7 days' prior notice that Your account is overdue, in accordance with Section 13.2 (Manner of Giving Notice), before suspending services to You.

6.5. Payment Disputes. We shall not exercise Our rights under Section 6.3 (Overdue Charges) or 6.4 (Suspension of Service and Acceleration) if You are disputing the applicable charges reasonably and in good faith and are cooperating diligently to resolve the dispute.

6.6. Taxes. Unless otherwise stated, Our fees do not include any taxes, levies, duties or similar governmental assessments of any nature, including but not limited to value-added, sales, use or withholding taxes, assessable by any local, state, provincial, federal or foreign jurisdiction (collectively, "Taxes"). You are responsible for paying all Taxes associated with Your purchases hereunder. If We have the legal obligation to pay or collect Taxes for which You are responsible under this paragraph, the appropriate amount shall be invoiced to and paid by You, unless You provide Us with a valid tax exemption certificate authorized by the appropriate taxing authority. For clarity, We are solely responsible for taxes assessable against it based on Our income, property and employees.

7. PROPRIETARY RIGHTS

7.1. Reservation of Rights in Services. Subject to the limited rights expressly granted hereunder, We reserve all rights, title and interest in and to the Services, including all related intellectual property rights. No rights are granted to You hereunder other than as expressly set forth herein.

7.2. Restrictions. You shall not (i) permit any third party to access the Services except as permitted herein or in an Order Form, (ii) create derivate works based on the Services except as authorized herein, (iii) copy, frame or mirror any part or content of the Services, other than copying or framing on Your own intranets or otherwise for Your own internal business purposes, (iv) reverse engineer the Services, or (v) access the Services in order to (a) build a competitive product or service, or (b) copy any features, functions or graphics of the Services.

7.3. Your Applications and Code. If You, a third party acting on Your behalf, or a User creates applications or program code using the Services, You authorize Us to host, copy, transmit, display and adapt such applications and program code, solely as necessary for Us to provide the Services in accordance with this Agreement. Subject to the above, We acquire no right, title or interest from You or Your licensors under this Agreement in or to such applications or program code, including any intellectual property rights therein.

7.4. Your Data. Subject to the limited rights granted by You hereunder, We acquire no right, title or interest from You or Your licensors under this Agreement in or to Your Data, including any intellectual property rights therein. 7.5. Suggestions. We shall have a royalty-free, worldwide, irrevocable, perpetual license to use and incorporate into the Services any suggestions, enhancement requests, recommendations or other feedback provided by You, including Users, relating to the operation of the Services.

7.6. Federal Government End Use Provisions. We provide the Services, including related software and technology, for ultimate federal government end use solely in accordance with the following: Government technical data and software rights related to the Services include only those rights customarily provided to the public as defined in this Agreement. This customary commercial license is provided in accordance with FAR 12.211 (Technical Data) and FAR 12.212 (Software) and, for Department of Defense transactions, DFAR 252.227-7015 (Technical Data –Commercial Items) and DFAR 227.7202-3 (Rights in Commercial Computer Software or Computer Software Documentation). If a government agency has a need for rights not conveyed under these terms, it must negotiate with Us to determine if there are acceptable terms for transferring such rights, and a mutually acceptable written addendum specifically conveying such rights must be included in any applicable contract or agreement.

8. CONFIDENTIALITY

8.1. Definition of Confidential Information. As used herein, "Confidential Information" means all confidential information disclosed by a party ("Disclosing Party") to the other party ("Receiving Party"), whether orally or in writing, that is designated as confidential or that reasonably should be understood to be confidential given the nature of the information and the circumstances of disclosure. Your Confidential Information shall include Your Data; Our Confidential Information shall include the Services; and Confidential Information of each party shall include the terms and conditions of this Agreement and all Order Forms, as well as business and marketing plans, technology and technical information, product plans and designs, and business processes disclosed by such party. However, Confidential Information (other than Your Data) shall not include any information that (i) is or becomes generally known to the public without breach of any obligation owed to the Disclosing Party, (ii) was known to the Receiving Party prior to its disclosure by the Disclosing Party without breach of any obligation owed to the Disclosing Party, (iii) is received from a third party without breach of any obligation owed to the Disclosing Party, or (iv) was independently developed by the Receiving Party.

8.2. Protection of Confidential Information. The Receiving Party shall use the same degree of care that it uses to protect the confidentiality of its own confidential information of like kind (but in no event less than reasonable care) (i) not to use any Confidential Information of the Disclosing Party for any purpose outside the scope of this Agreement, and (ii) except as otherwise authorized by the Disclosing Party in writing, to limit access to Confidential

Information of the Disclosing Party to those of its and its Affiliates' employees, contractors and agents who need such access for purposes consistent with this Agreement and who have signed confidentiality agreements with the Receiving Party containing protections no less stringent than those herein. Neither party shall disclose the terms of this Agreement or any Order Form to any third party other than its Affiliates and their legal counsel and accountants without the other party's prior written consent.

8.3. Compelled Disclosure. The Receiving Party may disclose Confidential Information of the Disclosing Party if it is compelled by law to do so, provided the Receiving Party gives the Disclosing Party prior notice of such compelled disclosure (to the extent legally permitted) and reasonable assistance, at the Disclosing Party's cost, if the Disclosing Party wishes to contest the disclosure. If the Receiving Party is compelled by law to disclose the Disclosing Party's Confidential Information as part of a civil proceeding to which the Disclosing Party is a party, and the Disclosing Party is not contesting the disclosure, the Disclosing Party will reimburse the Receiving Party for its reasonable cost of compiling and providing secure access to such Confidential Information.

9. WARRANTIES AND DISCLAIMERS

9.1. Our Warranties. We warrant that (i) We have validly entered into this Agreement and have the legal power to do so, (ii) the Services shall perform materially in accordance with the User Guide, (iii) subject to Section 5.3 (Integration with Non-Salesforce.com Services), the functionality of the Services will not be materially decreased during a subscription term, and (iv) We will not transmit Malicious Code to You, provided it is not a breach of this subpart (iv) if You or a User uploads a file containing Malicious Code into the Services and later downloads that file containing Malicious Code. For any breach of a warranty above, Your exclusive remedy shall be as provided in Section 12.3 (Termination for Cause) and Section 12.4 (Refund or Payment upon Termination) below.

9.2. Your Warranties. You warrant that You have validly entered into this Agreement and have the legal power to do so.

9.3. Disclaimer. EXCEPT AS EXPRESSLY PROVIDED HEREIN, NEITHER PARTY MAKES ANY WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, AND EACH PARTY SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES, INCLUDING ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW.

9.4. Non-GA Services. From time to time We may invite You to try, at no charge, Our products or services that are not generally available to Our customers ("Non-GA Services"). You may accept or decline any such trial in Your sole discretion. Any Non-GA Services will be clearly designated as beta, pilot, limited release, developer preview, nonproduction or by a

description of similar import. Non-GA Services are provided for evaluation purposes and not for production use, are not supported, may contain bugs or errors, and may be subject to additional terms. NON-GA SERVICES ARE NOT CONSIDERED "SERVICES" HEREUNDER AND ARE PROVIDED "AS IS" WITH NO EXPRESS OR IMPLIED WARRANTY. We may discontinue Non-GA Services at any time in Our sole discretion and may never make them generally available.

10. MUTUAL INDEMNIFICATION

10.1. Indemnification by Us. We shall defend You against any claim, demand, suit, or proceeding made or brought against You by a third party alleging that the use of the Services as permitted hereunder infringes or misappropriates the intellectual property rights of a third party (a "Claim Against You"), and shall indemnify You for any damages, attorney fees and costs finally awarded against You as a result of, and for amounts paid by You under a court-approved settlement of, a Claim Against You; provided that You (a) promptly give Us written notice of the Claim Against You; (b) give Us sole control of the defense and settlement of the Claim Against You (provided that We may not settle any Claim Against You unless the settlement unconditionally releases You of all liability); and (c) provide to Us all reasonable assistance, at Our expense. In the event of a Claim Against You, or if We reasonably believe the Services may infringe or misappropriate, We may in Our discretion and at no cost to You (i) modify the Services so that they no longer infringe or misappropriate, without breaching Our warranties under “Our Warranties” above, (ii) obtain a license for Your continued use of the Services in accordance with this Agreement, or (iii) terminate Your User subscriptions for such Services upon 30 days’ written notice and refund to You any prepaid fees covering the remainder of the term of such User subscriptions after the effective date of termination.

10.2. Indemnification by You. You shall defend Us against any claim, demand, suit or proceeding made or brought against Us by a third party alleging that Your Data, or Your use of the Services in breach of this Agreement, infringes or misappropriates the intellectual property rights of a third party or violates applicable law (a "Claim Against Us"), and shall indemnify Us for any damages, attorney fees and costs finally awarded against Us as a result of, or for any amounts paid by Us under a court-approved settlement of, a Claim Against Us; provided that We (a) promptly give You written notice of the Claim Against Us; (b) give You sole control of the defense and settlement of the Claim Against Us (provided that You may not settle any Claim Against Us unless the settlement unconditionally releases Us of all liability); and (c) provide to You all reasonable assistance, at Your expense.

10.3. Exclusive Remedy. This Section 10 (Mutual Indemnification) states the indemnifying party’s sole liability to, and the indemnified party’s exclusive remedy against, the other party for any type of claim described in this Section.

11. LIMITATION OF LIABILITY

11.1. Limitation of Liability. NEITHER PARTY'S LIABILITY WITH RESPECT TO ANY SINGLE INCIDENT ARISING OUT OF OR RELATED TO THIS AGREEMENT (WHETHER IN CONTRACT OR TORT OR UNDER ANY OTHER THEORY OF LIABILITY) SHALL EXCEED THE LESSER OF $500,000 OR THE AMOUNT PAID BY YOU HEREUNDER IN THE 12 MONTHS PRECEDING THE INCIDENT, PROVIDED THAT IN NO EVENT SHALL EITHER PARTY'S AGGREGATE LIABILITY ARISING OUT OF OR RELATED TO THIS AGREEMENT (WHETHER IN CONTRACT OR TORT OR UNDER ANY OTHER THEORY OF LIABILITY) EXCEED THE TOTAL AMOUNT PAID BY YOU HEREUNDER. THE FOREGOING SHALL NOT LIMIT YOUR PAYMENT OBLIGATIONS UNDER SECTION 6 (FEES AND PAYMENT FOR PURCHASED SERVICES).

11.2. Exclusion of Consequential and Related Damages. IN NO EVENT SHALL EITHER PARTY HAVE ANY LIABILITY TO THE OTHER PARTY FOR ANY LOST PROFITS OR REVENUES OR FOR ANY INDIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL, COVER OR PUNITIVE DAMAGES HOWEVER CAUSED, WHETHER IN CONTRACT, TORT OR UNDER ANY OTHER THEORY OF LIABILITY, AND WHETHER OR NOT THE PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE FOREGOING DISCLAIMER SHALL NOT APPLY TO THE EXTENT PROHIBITED BY APPLICABLE LAW.

12. TERM AND TERMINATION

12.1. Term of Agreement. This Agreement commences on the date You accept it and continues until all User subscriptions granted in accordance with this Agreement have expired or been terminated. If You elect to use the Services for a free trial period and do not purchase a subscription before the end of that period, this Agreement will terminate at the end of the free trial period. 12.2. Term of Purchased User Subscriptions. User subscriptions purchased by You commence on the start date specified in the applicable Order Form and continue for the subscription term specified therein. Except as otherwise specified in the applicable Order Form, all User subscriptions shall automatically renew for additional periods equal to the expiring subscription term or one year (whichever is shorter), unless either party gives the other notice of non-renewal at least 30 days before the end of the relevant subscription term. The per-unit pricing during any such renewal term shall be the same as that during the prior term unless We have given You written notice of a pricing increase at least 60 days before the end of such prior term, in which case the pricing increase shall be effective upon renewal and thereafter. Any such pricing increase shall not exceed 7% of the pricing for the relevant Services in the immediately prior subscription term, unless the pricing in such prior term was designated in the relevant Order Form as promotional or one-time.

12.3. Termination for Cause. A party may terminate this Agreement for cause: (i) upon 30 days written notice to the other party of a material breach if such breach remains uncured at

the expiration of such period, or (ii) if the other party becomes the subject of a petition in bankruptcy or any other proceeding relating to insolvency, receivership, liquidation or assignment for the benefit of creditors.

12.4. Refund or Payment upon Termination. Upon any termination for cause by You, We shall refund You any prepaid fees covering the remainder of the term of all subscriptions after the effective date of termination. Upon any termination for cause by Us, You shall pay any unpaid fees covering the remainder of the term of all Order Forms after the effective date of termination. In no event shall any termination relieve You of the obligation to pay any fees payable to Us for the period prior to the effective date of termination.

12.5. Return of Your Data. Upon request by You made within 30 days after the effective date of termination of a Purchased Services subscription, We will make available to You for download a file of Your Data in comma separated value (.csv) format along with attachments in their native format. After such 30-day period, We shall have no obligation to maintain or provide any of Your Data and shall thereafter, unless legally prohibited, delete all of Your Data in Our systems or otherwise in Our possession or under Our control.

12.6. Surviving Provisions. Section 6 (Fees and Payment for Purchased Services), 7 (Proprietary Rights), 8 (Confidentiality), 9.3 (Disclaimer), 10 (Mutual Indemnification), 11 (Limitation of Liability), 12.4 (Refund or Payment upon Termination), 12.5 (Return of Your Data), 13 (Who You Are Contracting With, Notices, Governing Law and Jurisdiction) and 14 (General Provisions) shall survive any termination or expiration of this Agreement.

13. WHO YOU ARE CONTRACTING WITH, NOTICES, GOVERNING LAW AND JURISDICTION

13.1. General. Who You are contracting with under this Agreement, who You should direct notices to under this Agreement, what law will apply in any lawsuit arising out of or in connection with this Agreement, and which courts can adjudicate any such lawsuit, depend on where You are domiciled.

If You are domiciled in:	You are contracting with:	Notices should be addressed to:	The governing law is:	The courts having exclusive jurisdiction are:
The United States of America, Mexico or a Country in Central or South America or the Caribbean	salesforce.com, inc., a Delaware corporation	The Landmark @ One Market, Suite 300, San Francisco, California, 94105, U.S.A., attn: VP, Worldwide Sales Operations Fax: +1-415-901-7040	California and controlling United States federal law	San Francisco, California, U.S.A.
Canada	salesforce.com Canada Corporation, a Nova Scotia corporation	The Landmark @ One Market, Suite 300, San Francisco, California, 94105, U.S.A., attn: VP, Worldwide Sales Operations Fax: +1-415-901-7040	Ontario and controlling Canadian federal law	Toronto, Ontario, Canada

If You are domiciled in:	You are contracting with:	Notices should be addressed to:	The governing law is:	The courts having exclusive jurisdiction are:
A Country in Europe, the Middle East or Africa	salesforce.com Sàrl, a Switzerland private limited liability company	Route de la Longeraie 9, Morges, 1110, Switzerland, attn: Director, EMEA Sales Operations Fax +41-21-6953701	Switzerland	Switzerland
Japan	Kabushiki Kaisha Salesforce.com, a Japan corporation	Roppongi Hills Mori Tower 39F, 6-10-1 Roppongi, Minato-ku, Tokyo 106-6139, Japan, attn: Director, Japan Sales Operations Fax +81-3-5793-8302	Japan	Tokyo, Japan
A Country in Asia or the Pacific region, other than Japan	Salesforce.com Singapore Pte Ltd, a Singapore private limited company	9 Temasek Boulevard #40-01, Suntec Tower 2, Singapore, 038989, attn: Director, APAC Sales Operations Fax +65 6302 5777	Singapore	Singapore

13.2. Manner of Giving Notice. Except as otherwise specified in this Agreement, all notices, permissions and approvals hereunder shall be in writing and shall be deemed to have been given upon: (i) personal delivery, (ii) the second business day after mailing, (iii) the second

business day after sending by confirmed facsimile, or (iv) the first business day after sending by email (provided email shall not be sufficient for notices of termination or an indemnifiable claim). Billing-related notices to You shall be addressed to the relevant billing contact designated by You. All other notices to You shall be addressed to the relevant Services system administrator designated by You.

13.3. Agreement to Governing Law and Jurisdiction. Each party agrees to the applicable governing law above without regard to choice or conflicts of law rules, and to the exclusive jurisdiction of the applicable courts above.

13.4. Waiver of Jury Trial. Each party hereby waives any right to jury trial in connection with any action or litigation in any way arising out of or related to this Agreement.

14. GENERAL PROVISIONS

14.1. Export Compliance. The Services, other technology We make available, and derivatives thereof may be subject to export laws and regulations of the United States and other jurisdictions. Each party represents that it is not named on any U.S. government denied-party list. You shall not permit Users to access or use Services in a U.S.-embargoed country (currently Cuba, Iran, North Korea, Sudan or Syria) or in violation of any U.S. export law or regulation.

14.2. Anti-Corruption. You have not received or been offered any illegal or improper bribe, kickback, payment, gift, or thing of value from any of Our employees or agents in connection with this Agreement. Reasonable gifts and entertainment provided in the ordinary course of business do not violate the above restriction. If You learn of any violation of the above restriction, You will use reasonable efforts to promptly notify Our Legal Department (legalcompliance@salesforce.com).

14.3. Relationship of the Parties. The parties are independent contractors. This Agreement does not create a partnership, franchise, joint venture, agency, fiduciary or employment relationship between the parties.

14.4. No Third-Party Beneficiaries. There are no third-party beneficiaries to this Agreement.

14.5. Waiver. No failure or delay by either party in exercising any right under this Agreement shall constitute a waiver of that right.

14.6. Severability. If any provision of this Agreement is held by a court of competent jurisdiction to be contrary to law, the provision shall be modified by the court and interpreted so as best to accomplish the objectives of the original provision to the fullest extent permitted by law, and the remaining provisions of this Agreement shall remain in effect.

14.7. Attorney Fees. You shall pay on demand all of Our reasonable attorney fees and other costs incurred by Us to collect any fees or charges due Us under this Agreement following Your breach of Section 6.2 (Invoicing and Payment).

14.8. Assignment. Neither party may assign any of its rights or obligations hereunder, whether by operation of law or otherwise, without the prior written consent of the other party (not to be unreasonably withheld). Notwithstanding the foregoing, either party may assign this Agreement in its entirety (including all Order Forms), without consent of the other party, to its Affiliate or in connection with a merger, acquisition, corporate reorganization, or sale of all or substantially all of its assets not involving a direct competitor of the other party. A party's sole remedy for any purported assignment by the other party in breach of this paragraph shall be, at the non-assigning party's election, termination of this Agreement upon written notice to the assigning party. In the event of such a termination, We shall refund to You any prepaid fees covering the remainder of the term of all subscriptions after the effective date of termination. Subject to the foregoing, this Agreement shall bind and inure to the benefit of the parties, their respective successors and permitted assigns.

14.9. Entire Agreement. This Agreement, including all exhibits and addenda hereto and all Order Forms, constitutes the entire agreement between the parties and supersedes all prior and contemporaneous agreements, proposals or representations, written or oral, concerning its subject matter. No modification, amendment, or waiver of any provision of this Agreement shall be effective unless in writing and either signed or accepted electronically by the party against whom the modification, amendment or waiver is to be asserted. However, to the extent of any conflict or inconsistency between the provisions in the body of this Agreement and any exhibit or addendum hereto or any Order Form, the terms of such exhibit, addendum or Order Form shall prevail. Notwithstanding any language to the contrary therein, no terms or conditions stated in Your purchase order or other order documentation (excluding Order Forms) shall be incorporated into or form any part of this Agreement, and all such terms or conditions shall be null and void.

Annex 2: TWINFIELD GENERAL TERMS AND CONDITIONS

GENERAL

1. DEFINITIONS

1.1 In these terms and conditions, the following capitalised terms have the meaning set forth hereunder:

Administration: financial records which are kept with the use of the Webservice;

Environment: an environment in the Webservice dedicated to Subscriber;

Order Form: the electronic order form on Twinfield's website which has been completed and submitted to Twinfield by Subscriber or any other document in which these terms and conditions have been declared applicable;

Parties: Subscriber and Twinfield;

Price List: Twinfield's price list for the use of the Webservice and associated services, as amended from time to time;

Report: a report from an User to Twinfield on a problem relating to the Webservice or a question about the use or the implementation of the Webservice;

Servers: a collection of dedicated computers and related hardware managed by Twinfield, upon which is installed webserver software, support software or database software for providing the Webservice via the Internet;

Service Hours: the opening hours of Twinfield's helpdesk, being Monday to Friday 07.00 - 17.00 hours British time;

Special Conditions: any special terms and conditions which may have been agreed between the Parties;

Subscriber: the natural or legal person who has submitted the Order Form and has therewith entered into the Subscription Agreement;

Subscription: a subscription to the Webservice giving Subscriber the rights set forth in Article 3.1;

Subscription Agreement: the agreement referred to in Article 2.1;

Subscription Conditions: the terms and conditions published on Twinfield's website which apply to each of the Subscriptions of Subscriber;

Super User: an User who has been appointed by Subscriber as administrator of the Environment;

Support: the provision of customer support pursuant to Article 16;

Twinfield: Twinfield UK Accounting Limited, a limited liability company incorporated in England with registration number 07089421 and its registered office at Brierly Place, New London Road, Chelmsford, Essex CM2 0AP;

User: a natural person who is authorised by Subscriber to use the Webservice on behalf of Subscriber and has access to one or more Administrations;

Webservice: the on-line web application for bookkeeping supplied by Twinfield.

2. APPLICABILITY

2.1 These terms and conditions, together with the Order Form, the Subscription Conditions and any Special Conditions constitute the Subscription Agreement between Subscriber and Twinfield and are legally binding on Subscriber and Twinfield. The Subscription Agreement governs each Subscription taken out by Subscriber and all services rendered by Twinfield to subscriber to the exclusion of any other terms that Subscriber seeks to impose or incorporate, or which are implied by trade, customer, practice or course of dealing.

2.2 The documents constituting the Subscription Agreement have the following order of priority: the Order Form; the Special Conditions (if any); the Subscription Conditions; these terms and conditions. In case of conflict between those documents, the document with the highest priority will prevail.

2.3 Twinfield may make amendments to the Subscription Agreement. In case of an amendment, Twinfield will give Subscriber at least 30 days notice thereof. An amendment will be considered to be accepted by Subscriber and will enter into force on the date determined by Twinfield if Subscriber

does not reject the Amendment within 30 days following the notification thereof. If Subscriber rejects the amendment, Twinfield will be entitled to terminate the Subscription Agreement by giving at least 30 days notice of termination with effect from the end of a calendar month.

3. SUBSCRIPTIONS

3.1 A Subscription entitles Subscriber to give one User access to the Webservice in order to keep at most 5 Administrations for Subscriber or its affiliated companies. The functions offered under a Subscription and the rights attached to a Subscription depend on the subscription level. Subscriber may give access to its Administration(s) in order to inspect those Administrations to an accountancy firm, accounting office or other similar service provider. Twinfield may require that such accountancy firm or service provider meets certain standards of competence set by Twinfield.

3.2 If Subscriber wishes to give access to its Administrations to more than one User or wishes to give a User access to more than 5 Administrations, it must take out one additional Subscription for each additional User and for each 5 additional Administrations to which a User will get access.

3.3 Subscriber acknowledges and agrees that the Webservice is provided on an "as is" basis.

3.4 Twinfield will, at the written request of Subscriber, create Administrations, Users and Subscriptions for Subscriber, or remove Administrations, Users or Subscriptions from the Webservice. If the number of Users or Administrations or the functions of the Webservice used by a User does not correspond with the Subscriptions of Subscriber, Twinfield may charge Subscriber for one additional Subscription for each additional User and for each additional 5 Administrations to which a User has access. In addition, Twinfield may charge Subscriber in respect of each User for the subscription level which corresponds with the most comprehensive functions of the Webservice used by or made available to such User.

3.5 With the exception of Article 3.1, Subscriber may only register its officers, employees and other persons employed or engaged by Subscriber as Users. On request of Twinfield Subscriber must demonstrate that an User meets those requirements. The burden of proof that a User meets these requirements rests on Subscriber.

3.6 If Subscriber meets the requirements of Twinfield which apply to first level subscribers it may opt for an Environment. The Environment will be dedicated to Subscriber for maintaining its Administrations. Subscriber may create Administrations, Super Users and Users in the Environment. Subscriber shall register in the Environment to which Administrations each User has access and which Subscription(s) apply to each Users. If Subscriber has obtained an Environment it may not open or maintain Administrations outside the Environment. Article 3.4 applies accordingly to Users and Administrations created in the Environment and the Subscriptions registered in the Environment.

4. INDEBTEDNESS OF SUBSCRIPTION FEES

4.1 The fees for Subscriptions are charged on a monthly basis and are payable in arrears. The fees for Subscriptions are based on the maximum number of Subscriptions of Subscriber and the most comprehensive Subscription for each User during the relevant month.

4.2 Twinfield will be entitled to suspend one or more User's access to the Webservice or the access of all Users to one or more Administrations if the number of Users or Administrations, the number of Administrations to which a User has access, or the functions used by a User do not correspond with the Subscriptions of Subscriber. Twinfield will be entitled to suspend a User's access to the Webservice if it has prima facie evidence that such User does not meet the requirements set forth in Article 3.5. Twinfield is entitled to remove Administration if such Administration is not related to the business of Subscriber or an affiliated company of Subscriber.

4.3 Subscriber must give timely notice to Twinfield if it wishes to terminate a Subscription or remove an Administration or User from the Webservice. If Subscriber has obtained an Environment it will be responsible for the timely removal from the Environment of Subscriptions and Administrations that are no longer used and Users who

it no longer wish to admit to the Environment or certain Administrations. Subscriber shall be charged and pay for each Subscription until such Subscription and the relevant Administrations and Users have been removed from the Webservice or the Environment and the minimum term and the notice period of the Subscription have expired.

5. PRICING AND TERMS OF PAYMENT

5.1 The fees to be paid by Subscriber to Twinfield for the use of the Webservice and additional services are to be Twinfield's list prices as specified in the Price List. The prices for services which are not specified in the Price List will be determined by agreement.

5.2 Twinfield is entitled to increase its fees annually with the same percentage as the increase of the consumer prices during the prior calendar year as published by [ ] and to round up those prices to whole Great British Pounds.

5.3 Twinfield will send Subscriber an invoice each month for the use of the Webservice in the prior month. The fees for training sessions are due in advance. Consultancy services will be charged to and paid for by Subscriber after they have been provided. Consultancy services which are provided during more than one calendar month will be charged on a monthly basis in arrears. Twinfield may demand advance payment of the fees for consultancy services.

5.4 Subscriber shall pay Twinfield's invoices within 14 days from the date of invoice. If Subscriber disagrees with an invoice, it must give Twinfield notice thereof within 2 months following the invoice date. If no objection has been made against an invoice within this term, the indebtedness of the invoice amount by Subscriber will therewith be established. Time is of the essence for payment. A failure of Subscriber to pay any amount due to Twinfield in time shall be considered as a material breach of the Subscription Agreement.

5.5 Twinfield may request Subscriber to pay by direct debit. In case of such payment by direct debit, the amount of the invoice will be debited from Subscriber's account on the day of the invoice. If Subscriber does not agree to pay by direct debit or the direct debit entry fails or is not honoured, Twinfield will be entitled to charge an administration fee to Subscriber of at most GBP 5 per invoice.

5.6 All payments made by Subscriber will first be applied against the oldest of any outstanding invoices from Twinfield, irrespective of any other indication by Subscriber. Subscriber may not postpone payment or withhold payment of any amount due to Twinfield because of any set-off, counterclaim, abatement, or other reason.

5.7 Twinfield is authorised to read out, whether or not automatically, the user management data entered in the Environment and to use those data to ensure correct calculation and invoicing of the fee for the use of the Webservice to Subscriber. In addition, Twinfield has the right to check the numbers of Users, Administrations and Subscriptions maintained by Subscriber in the Webservice.

5.8 If Subscriber fails to pay Twinfield on the due date, Twinfield may without prejudice to any other right or remedy

a. charge interest on the overdue amount at the rate of 4% per annum above the base rate of the Bank of England from time-to-time. The interest period shall run from the due date of payment until receipt of the full amount by Twinfield, whether before or after judgment. Notwithstanding the foregoing, Twinfield may in the alternative claim interest at its discretion under the Late Payment of Commercial Debts (Interest) Act 1998; and

b. suspend all provision of the Webservice to Subscriber until payment has been made in full.

5.9 All sums payable by Subscriber to Twinfield shall become due immediately on the termination of the Subscription Agreement, despite any other provision. This Article 5.9 is without prejudice to any other right of Twinfield under the law or the Subscription Agreement.

6. LIABILITY

6.1 This Article 6 sets out the entire financial liability of Twinfield (including any liability for the acts or omissions of its employees, agents and sub-contractors) to Subscriber in respect of:

a. any breach of the Subscription Agreement;

b. any use made by Subscriber of the Webservice;

c. any training given or service provided by Twinfield; and

d. any representation, statement or tortious act or omission (including negligence) arising under or in

connection with the Subscription Agreement or the supply of the Webservice.

6.2 Except as expressly and specifically provided in these terms and conditions, all warranties, representations, conditions and all other terms of any kind whatsoever implied by statute or common law are, to the fullest extent permitted by applicable law, excluded from the Subscription Agreement.

6.3 Nothing in the Subscription Agreement excludes the liability of Twinfield:

a. for death or personal injury caused by Twinfield's negligence; or

b. for fraud or fraudulent misrepresentation of Twinfield; or

c. for damage caused by an intentional act of gross negligence by directors or senior management of Twinfield.

6.4 SUBJECT TO ARTICLE 6.3:

a. Twinfield shall not be liable whether in tort (including for negligence or breach of statutory duty), contract, misrepresentation, restitution or otherwise for any loss of profits, loss of business, depletion of goodwill or similar losses, or loss or corruption of data or information, or pure economic loss, or for any special, indirect or consequential loss, costs, damages, charges or expenses however arising under the Subscription Agreement; and

b. Twinfield's total aggregate liability in contract, tort (including negligence), breach of statutory duty, misrepresentation, restitution or otherwise, arising in connection with the performance or lack of performance of the Subscription Agreement or the supply of the Webservice shall be limited to the fees paid by Subscriber to Twinfield for the use of the Webservice during the 12 months period preceding the event which caused the loss or damage.

6.5 Apart from Twinfield, each of its affiliated companies, employees, agents and sub-contractors may invoke the limitation of liability set forth in this Article 6. Save and except as expressly provided in this Article 6.5 in respect of the parties mentioned in this article 6.5 and for the benefit of applying the limit referred to in this Article 6.5, a person who is not a party to the Subscription Agreement shall not have any rights under or in connection with it by value of the Contracts (Rights of Third Parties) Act 1999

6.6 This Article 6 shall survive termination of the Subscription Agreement.

7. INDEMNITIES

7.1 Subscriber shall indemnify Twinfield against all liabilities, costs, expenses, damages and losses (including legal costs and expenses) suffered or incurred by Twinfield arising out of or in connection with:

a. any breach of Articles 9.5, 11.5, 12.5, 12.7, 12.10, 12.13, 15.1, 15.2 and 15.6;

b. any third party claim arising out of or in connection with Subscriber's unauthorized use or adaptation of the Webservice;

c. and/or exchanged by Subscriber or Users is unlawful.

7.2 This Article 7 shall survive termination of this Agreement.

8. IP RIGHTS AND RIGHTS IN THE ADMINISTRATIONS

8.1 Subscriber acknowledges and agrees that all intellectual property rights in the Webservice, including (without limitation) the functional and technical design, the lay out, the programming, the structure of the database, the functionalities and the source codes of the Webservice, all related documents and all goodwill exclusively belong to Twinfield or its licensors. The provision of the Webservice or any related product or service does not imply any transfer of intellectual property rights to Subscriber.

8.2 All rights of whatever nature in the data in an Administration belong to the Subscriber.

9. TERM AND TERMINATION

9.1 A Subscription is entered into for an indefinite period and shall continue for a minimum period of one year, unless terminated as provided in Article 9.3. Either Party may terminate the Subscription Agreement for convenience after the minimum period has lapsed by giving 30 days written notice to the other Party with effect from the end of a calendar month.

9.2 The Subscription Agreement become effective on the date of the submission of the Order Form by Subscriber

and terminates by force of law upon the termination of all Subscriptions.

9.3 Without prejudice to any other rights or remedies to which the Parties may be entitled, either Party may terminate this Agreement immediately without liability to the other Party if:

a. the other Party commits a material breach of any of the terms of the Subscription Agreement and (if such a breach is remediable) fails to remedy that breach within 30 days of that Party being notified in writing of the breach;

b. the other Party commits persistent breaches of the Subscription Agreement (such breaches having been notified in writing), so as to reasonably justify the opinion that its conduct is inconsistent with it having the intention or ability to abide by the Subscription Agreement;

c. the other Party suspends, or threatens to suspend, payment of its debts or is unable to pay its debts as they fall due or admits inability to pay its debts or (being a company) is deemed unable to pay its debts within the meaning of Section 123 of the Insolvency Act 1986, or (being an individual) is deemed either as unable to pay its debts or as having no reasonable prospect of doing so, in either case, within the meaning of Section 268 of the Insolvency Act 1986, or (being a partnership) has any partner to whom any of the foregoing apply;

d. an order is made or a resolution is passed for the winding up of the other Party (being a company), or circumstances arise which entitle a court of competent jurisdiction to make a winding-up order in relation to the other Party;

e. an order is made for the appointment of an administrator to manage the affairs, business and property of the other Party, or documents are filed with a court of competent jurisdiction for the appointment of an administrator of the other Party, or notice of intention to appoint an administrator (or administrative receiver as the case may be) is given by the other Party or a qualifying floating charge holder (as defined in paragraph 14 of Schedule B1 to the Insolvency Act 1986);

f. a receiver is appointed of any of the other Party's assets or undertaking, or if circumstances arise which entitle a court of competent jurisdiction or a creditor to appoint a receiver or manager of the other Party, or if any other person takes possession of or sells the other Party's assets;

g. the other Party makes an arrangement or composition with its creditors, or makes an application to a court of competent jurisdiction for the protection of its creditors in any way;

h. the other Party (being an individual) is the subject of a bankruptcy petition or order.

i. the other Party ceases its business;

j. the other Party takes or suffers any similar or analogous action in any foreign jurisdiction in consequence of dept.

9.4 In case of termination of the Subscription Agreement all Subscriptions shall automatically end.

9.5 On termination of the Subscription Agreement for any reason:

a. Subscriber shall no longer have access to the Webservice;

b. the right of Subscriber to use the Webservice lapses immediately and Subscriber shall cease all use of the Webservice;

c. Twinfield will no longer be responsible for saving the data in the Administrations and the Environment. The data referred to in Article 21.2 shall be made available to Subscriber, provided that Subscriber makes a written request to that effect to Twinfield within one month after the effective date of the termination of the Subscription Agreement, in which case Article 21.2 shall apply;

d. the accrued rights of the Parties as at termination, or the continuation after termination of any provision expressly stated to survive or implicitly surviving termination, shall not be affected or prejudiced.

9.6 In case of the termination of an Administration or all Subscriptions in respect of an Administration, Twinfield will no longer be responsible for saving the data in such Administration. The data in the terminated Administration referred to in Article 21.2 shall be made available to Subscriber, provided that Subscriber makes a written request to that effect to Twinfield within one month after the effective data of the termination of the Administration, in which case Article 21.2 shall apply.

9.7 Twinfield will be entitled to charge a fee for saving data after termination of an Administration or all Subscriptions in respect of an Administration.

10. FORCE MAJEURE

10.1 Twinfield shall not be in breach of the Subscription Agreement, nor liable for any failure or delay in performance of its obligations under the Subscription Agreement arising from or attributable to force majeure. Force majeure includes a failure of a supplier of Twinfield, government measures or instructions, strikes, power outs, internet or telephone interruptions and other circumstances beyond Twinfield's reasonable control.

10.2 If any delaying event under Article 10.1 continues for a period of 60 days of more, either Party may terminate the Subscription Agreement by giving written notice to the other Party of its intention to terminate the Subscription Agreement at the expiry of 14 days from the date of such notice, unless in the meantime the delay in performance has ended.

11. MISCELLANEOUS

11.1 Subscriber consents to Twinfield indicating in advertisements and brochures that Subscriber makes use of the Webservice and using Subscriber's name and logo for that purpose.

11.2 Subscriber consents to receiving messages, newsletters, advertisements and other communications from Twinfield by e-mail, unless it informs Twinfield via Twinfield's website or by e-mail to cso@twinfield.com that it does not wish to receive such communications.

11.3 All notices and other communications by Subscriber to Twinfield must be in writing and can be sent by e-mail to cso@twinfield.com. Subscriber will bear the burden of proof that an e-mail or other written communication has been received by Twinfield. All notices to Subscriber may be given by e-mail or a communication in the Webservice.

11.4 No amendment or variation of the Subscription Agreement shall be effective unless it is in writing and signed by both Parties or in accordance with Article 2.3.

11.5 Subscriber may not, without the prior written consent of Twinfield, assign, transfer, or pledge its rights and obligations under the Subscription Agreement, or allow a third party to make use thereof.

11.6 Twinfield may at any time assign, transfer, or in any other manner dispose of any or all of its rights and obligations under the Subscription Agreement. Twinfield may sub-contract or delegate any or all of its obligations under the Subscription Agreement to a third party.

11.7 The Subscription Agreement constitutes the whole agreement between the Parties and supersedes all previous agreements between the Parties relating to its subject matter.

11.8 If any court or competent authority finds that any provision of the Subscription Agreement (or part of any provision) is invalid, illegal or unenforceable, that provision or part-provision shall, to the extent required, be deemed to be deleted, and the validity and enforceability of the other provisions of the Subscription Agreement shall not be affected.

11.9 No failure or delay by a Party to exercise any right or remedy provided under the Subscription Agreement or by law shall constitute a waiver of such right or remedy, nor shall it preclude or restrict the further exercise of such right or remedy. No single or partial exercise of such right or remedy shall preclude or restrict the further exercise of that or any other right or remedy.

11.10 A person who is not a party to the Subscription Agreement shall not have any rights under or in connection with it by virtue of the Contracts (Rights of Third Parties) Act 1999.

11.11 The Subscription Agreement and any dispute or claim arising out of or in connection with it or its subject matter or formation (including non-contractual disputes or claims) shall be governed by and construed in accordance with the laws of England and Wales.

11.12 The Parties irrevocably agree that the courts of England and Wales shall have exclusive jurisdiction to settle any dispute or claim that arises out of or in connection with the Subscription Agreement or its subject matter or formation (including non-contractual disputes or claims).

USE OF THE WEBSERVICE

12. PROVISION AND USE OF THE WEBSERVICE

12.1 The Webservice is offered from a central location as a shared generic solution. The Webservice is not specifically maintained for Subscriber.

12.2 Twinfield will send Subscriber the URL of the Webservice, a user code and a password within 5 working days after the date on which the Subscription Agreement becomes effective. Subscriber can use these to instruct Twinfield to register other Subscriptions, Administrations and Users.

12.3 If Subscriber has obtained an Environment, Subscriber will use the Webservice for keeping its Administrations and for managing those Administrations and the Environment. In case of an Environment, Subscriber will only have access to the Environment and the Administrations in the Environment.

12.4 If a second user tries to log in to the Webservice with a combination of user code and password that is already being used, the session already in use will automatically be terminated.

12.5 The Environment will contain 2 template Administrations. Subscriber may open a maximum number of 5 template Administrations free of charge.

12.6 Twinfield has the right to modify the offered functionalities of the Webservice from time to time to improve or change the functionalities and correct errors. Twinfield will make every effort to solve errors in the Webservice, but does not warrant that all errors are corrected. If a modification results in a change in the functionality, Twinfield will give notice thereof via a communication in the Webservice or an e-mail to the Super User. No changes will be made or omitted for Subscribers or an individual Subscriber.

12.7 The Users determine which information is saved and/or exchanged using the Webservice. Twinfield has no knowledge of this information. Subscriber is responsible for ensuring that the information saved and/or exchanged by Users is lawful and does not breach the rights of third parties. Twinfield does not accept any liability whatsoever for the information saved and/or exchanged using the Webservice.

12.8 Twinfield is not responsible for the correctness of the data or the compliance by
Users with accounting regulations. Twinfield makes every effort to ensure that transactions entered by Users are correctly recorded and validated by the Webservice. However, information that is incorrectly entered by a User cannot be recognized as such by the Webservice and will consequently be incorrectly saved or recorded.

12.9 If it becomes apparent to Twinfield that the information that is saved in or exchanged via the Webservice is unlawful, then it will delete such information or block the access to it. In no case shall Twinfield be liable for damages resulting therefrom.

12.10 Twinfield, Subscriber and the Users are obliged to keep all user codes and passwords secret.

12.11 Twinfield is not liable for misuse or loss of user codes and passwords, and it may assume that the Users who login using a user code and password are actually the Users who have been authorized to do so by Subscriber. The moment Subscriber knows or has reason to suspect that user codes or passwords have fallen into the hands of unauthorized persons, it will immediately informed Twinfield thereof.

12.12 Each User can change her/his own password. Subscriber will endeavour to ensure that the Users change their password at least every 2 months.

12.13 Subscriber shall ensure that the Users carefully observe the user instructions and directions of Twinfield and are bound to the applicable practices of normal use of a webservice such as the Webservice. If the conduct of Subscriber or a User endangers the proper functioning of the Webservice, Twinfield will be entitled to block access to the Webservice by such User or all Users, without prior notice.

12.14 Twinfield applies no fixed limit to the quantity of data and/or master files that Subscriber or Users may process using the Webservice. However, this does not mean that Twinfield will permit an unlimited processing of such data or master files. In case of higher than average use of an Administration or the Environment compared to the number of Subscriptions being paid for, Twinfield will inform Subscriber thereof. When Subscriber does not reduce or cause the reduction of such use, Twinfield may impose a

reasonable increase in fees. If Subscriber does not agree to pay the higher fees, Twinfield has the right to terminate the Subscription Agreement at no cost with 30 days notice.

12.15 If Subscriber wishes to allow one or more Users to log in via a single sign-on functionality it needs to sign a declaration to be obtained from Twinfield. The use of a single sign-on functionality will be at the risk of Subscriber.

12.16 Twinfield is not permitted to use the data from the Environment or the Administrations, other than to provide services to Subscriber. Twinfield is permitted to use the data in anonymous form for statistical purposes. Twinfield is allowed to use a copy of the Environment in the acceptance environment to monitor the correct functioning of the Environment or to test the correct functioning of an update of the Webservice.

12.17 The Webservice will be regularly audited by registered EDP auditors (RE) from a reputable independent IT audit firm.

12.18 Subscriber is able to inspect in the Webservice which Users use a certain functionality.

13. TRAINING SESSIONS

13.1 Subscriber can register Users to attend a Twinfield training session on the use of the Webservice. If the number of registrations in the judgment of Twinfield gives reason to do so, Twinfield is permitted to reschedule the training session or to combine it with one or more other training sessions. Twinfield gives no warranty whatsoever regarding the content or result of the training. Subscriber accepts that the training will be given by Twinfield to the best of its ability.

13.2 The fees for attending a training session, the cancelation policy and other terms and conditions in respect of training sessions are published on Twinfield's website.

14. CONSULTANCY SERVICES

14.1 The Parties can separately and in writing agree on additional advisory and other services by Twinfield to Subscriber. Such services will be provided on a consulting basis. Twinfield warrants that it will use reasonable skill and care in the performance of such services, but does not warrant that it will achieve a specific result. Accordingly, Twinfield does not accept liability for failing to achieve a specific result.

14.2 If it is agreed that the consultancy services will be given in phases, Twinfield is authorized to defer the commencement of the services that form a part of a phase until Subscriber has approved the results of the preceding phase in writing.

14.3 Twinfield is only obliged to follow instructions by Subscriber regarding the performance of consultancy services if this is explicitly agreed in writing and does not require extra work, and provided that the instructions are reasonable and given in good time.

14.4 If an agreement to provide consultancy services is entered into with the view of having it performed by a specific person, Twinfield is nevertheless at all times authorized to replace this person with another person after notifying Subscriber.

15. PRIVACY, SECURITY AND CONFIDENTIALITY

15.1 Twinfield and all employees of Twinfield shall observe strict confidentiality in respect of all data in the Administrations and the Environment and all information that can be derived there from. The Parties undertake that they shall not at any time disclose to any person any confidential information concerning the business, affairs, customers, clients or suppliers of the other Party or of any member of the group of companies to which the other Party belongs, except as provided in this Article 15.

15.2 No Party shall use any other Party's confidential information for any purpose other than to perform its obligations under the Subscription Agreement.

15.3 Each Party may disclose the other Party's confidential information:

a. to those of its employees, officers, representatives or advisers who need to know such information for the purpose of carrying out the Party's obligations under the Subscription Agreement. Each Party shall ensure that its employees, officers, representatives or advisers to whom it discloses the other Party's confidential information comply with this Article 15; and

b. as may be required by law, court order or any governmental or regulatory authority.

15.4 Information will be regarded as confidential if such information is not generally available to the public, unless the

Party providing the information indicates such information as being non-confidential.

15.5 The use of the Webservice may involve processing personal data. It is the intention of the Parties that, for the purpose of the Data Protection Act 1998, Twinfield will be the data processor and Subscriber will be the data controller.

15.6 Subscriber shall strictly adhere to the Data Protection Act 1998 and shall ensure that it is entitled to transfer the relevant personal data to the Webservice for the purposes of saving and processing those data. Subscriber shall procure that the relevant third parties have been informed of, and have given their consent to, such use, processing, and transfer as required by all applicable data protection legislation.

15.7 All staff who act under the authority of Twinfield and have access to personal data will observe confidentiality with respect to those personal data.

15.8 Twinfield will take reasonable measures to protect the personal data saved or processed in the Webservice and shall strictly adhere to the Data Protection Act 1998. Twinfield will make reasonable effort to prevent unauthorised persons from accessing data of Subscriber. The information regarding these measures will be made available to Subscriber for inspection, to a limited and responsible extent, on Subscriber's request.

15.9 The data of Subscriber will only be saved and processed on one of the Servers, all of which are located in a country forming part of the European Economic Area (EEA).

15.10 Subscriber shall take reasonable measures to ensure that the Users will use the customary security software that should normally be installed on a computer, such as anti-virus, anti-spam, anti-spyware, anti-malware, anti-phishing and firewall software, as well as the security measures that Twinfield makes available.

15.11 This Article 15 shall survive termination of the Subscriber Agreement.

SERVICE LEVEL

16. SUPPORT

16.1 Subscriber has the right to Support for the use of the Webservice with respect to the functionality of the Webservice. Support is available during Service Hours. Twinfield can only offer Support if Subscriber uses operating systems that are supported by the manufacturer of the operating systems. Support comprises general assistance regarding the Webservice, including explanation of the documentation, help to allow Subscriber to get the Webservice working correctly and, if Subscriber has taken out a Subscription, verification and analysis of the correctness of the entered and processed data. Support does not extend to the full operation of functions when no training has been followed by the User, or the provision of implementation, training and consultancy services.

16.2 If Subscriber has obtained an Environment, it shall appoint at least one Super User. One of the Super Users will act as principal contact person with Twinfield. Twinfield may require that a Super User meets certain standards of competence set by Twinfield or attends certain training sessions. Articles 5 and 13 shall apply to those training sessions.

16.3 Support is provided via an online helpdesk function in the Webservice or by telephone. Twinfield will be entitled to offer telephone support as a phone paid service. Support by telephone will only be given during Service Hours and will only be available to Super Users. Twinfield will endeavou r to adequately answer questions, but does not warrant the correctness and/or completeness of the answers. Questions regarding the method of accounting or internal bookkeeping regulations will not be handled.

16.4 Users can send Reports to Twinfield via the online helpdesk in the Webservice.

16.5 Subscriber shall ensure that, before making a Report, Users will first put their questions in respect of the Webservice to a Super User and consult the knowledge base behind the questions mark in the Webservice.

16.6 Twinfield and third parties who are engaged by Twinfield may have access to the Environment and the Administrations for providing Support and may make those changes to the Environment and the Administrations as they deem necessary for solving a problem indicated in a Report.

16.7 Support is provided from an office of Twinfield. If assistance is desired at the location of Subscriber, a separate agreement must be made at the then applicable rate. Article 14 will apply to such agreement.

16.8 Twinfield is not liable for any failure to react to a Report due to the incorrect, incomplete or delayed sending and/or receipt of a Report submitted by a User, caused by the incomplete functioning of the telecom services or hardware of third parties and/or Subscriber.

16.9 Twinfield can freely choose which staff member deals with a Report. Subscriber cannot demand to be served by a specific person.

16.10 Subscriber can be charged by Twinfield for processing a Category 40 Report (as referred to in Article 17.1) If so, Twinfield will inform Subscriber in advance.

16.11 Subscriber can monitor in the Webservice how Twinfield follows up a Report.

17. RESPONSE TIMES

17.1 Reports have the following priority:

a. Category 10 Report: a report on the Webservice being entirely unreachable owing
to a fault on the part of Twinfield, or the Webservice having entirely stopped,
such that none of the functions are available;

b. Category 20 Report: a report on a problem that causes a serious application error,
which can endanger the progress of an essential processing period, but which
does not bring the entire Webservice to a stop;

c. Category 30 Report: a report on a minor problem in the Webservice that does not
require the immediate response of Twinfield;

d. Category 40 Report: all questions and requests for information regarding the use
or implementation of the Webservice.

17.2 The following response times apply within the Service Hours: Category 10 Reports: 2 hours, Category 20 Reports: 5 hours; Category 30 Reports: 8 hours; Category 40 Reports: 20 hours. In determining the response time, only Service Hours will be taken into account. Twinfield will decide in good faith which category applies to a Report.

18. ACCESSIBILITY

18.1 Twinfield will make every effort to ensure the accessibility of the Webservice by Subscriber for the purposes to which it is entitled.

18.2 Twinfield will provide a minimum level of accessibility (uptime) of the Webservice of 99.6% per month, with the exception of the exclusions as indicated in Article 20. The above mentioned percentage is measured over a calendar month and at the closest measuring point. Accessibility is understood to mean that the Webservice is available on the internet at the URL provided to Subscriber and is actually provided on the Servers. Accessibility is not understood to mean the existence of a working point-to-point connection between the systems of Subscriber and the Servers. Twinfield is not responsible for the systems at Subscriber and the connecting internet infrastructure.

18.3 The accessibility of the Webservice is measured every 3 minutes from at least 6 locations around the world. The current value of the accessibility can be retrieved using the login screen of the Webservice. The given values reflect the average minimum accessibility for the cumulative values of all the measuring locations around the world.

19. PERFORMANCE

19.1 Twinfield warrants it makes every effort to ensure that the Webservice works properly without any problems and that the speed is sufficient to be able to continuously work with it during the day. In this regard, the following measurement is used as an objective measuring assessment: the manual retrieval or saving of a document with two lines using an average computer via an internet connection of average speed in an environment with an average size is effected in two out of three cases within 1.5 seconds, where in the third case the time may not be longer than 2 seconds. Notwithstanding the foregoing, Twinfield:

a. does not warrant that Subscriber's use of the Webservice will be uninterrupted or error-free, nor that the Webservice will meet Subscriber's requirements; and

b. is not responsible for any delays, delivery failures, or any other loss or damage resulting from the transfer of data over communications networks and facilities, including the

internet, and Subscriber acknowledges that the Webservice may be subject to limitations, delays and other problems inherent in the use of such communications facilities.

19.2 Twinfield only warrants the performance indicated in Article 19.1 if and insofar as Subscriber satisfies the minimum system requirements specified by Twinfield from time to time, including the support of Internet Explorer, Firefox and other browsers that run under Windows, Apple Macintosh and Linux or other platforms. Moreover, Subscriber must have sufficient bandwidth. In this regard, it is assumed that at least 128 Kbit'sec (both download and upload) is available at all times for the workstation from where the Webservice is used, to be measured by an independent website such as www.speedtest.nl. However, it is not necessary for every individual workstation to have this bandwidth.

19.3 Twinfield is at all times authorized to change these minimum system requirements. In this case, Subscriber will be informed about this beforehand. If Subscriber does not satisfy these new requirements, the warranty in article 19.2 regarding performance -lapses.

19.4 The Webservice is a pure webservice. This means that the Webservice was not developed for use via Terminal Services or Citrix. Twinfield endeavours to support such constructions to the best of its ability.

19.5 The Webservice is offered from a location equipped to offer the Webservice in a professional manner according to the current state of the art, knowledge and customary and acceptable level of costs. This includes the physical protection of the premises, the prevention of access by unauthorized persons, 24/7 hardware-support, fire prevention, power backup and internet access security including a firewall, general security, data protection, and making reserve copies.

19.6 Twinfield will use reasonable commercial endeavours to monitor the data traffic from and to the Webservice and to respond within 30 minutes to unauthorised attempts by third parties to access the Webservice, to irregular traffic that cannot be handled by the Webservice, to harmful data traffic or other attempts to undermine the correct functioning of the Webservice. In such cases, Twinfield is authorized to block access to the Webservice.

20. EXCLUSIONS

20.1 Without prejudice to Article 19.1 sub a and b the service level set forth in Article 16 through 19 does not apply in the following situations:

a. during the regular maintenance windows. These will not be scheduled more than 2 times a month and will not commence before 23.00 hours Dutch time. Twinfield will inform Subscriber about such a maintenance window in writing at least 2 working days in advance;

b. in case of incidents resulting from or attributable to force majeure;

c. in case of any problem or disruption caused by an act of a User;

d. in case of the unavailability of the Webservice at the request of Subscriber and/or unavailability of the Webservice during work at the request of Subscriber;

e. if Twinfield needs the assistance of Subscriber to determine or isolate a problem or fault, and Subscriber does not provide such assistance;

f. if the Subscriber does not comply with the minimum system requirements set forth in Article19.2;

g. if the incident is caused by malfunctioning of the systems at Subscriber or the internet infrastructure.

21. BACK-UP AND OTHER SERVICES

21.1 Subscriber consents to a reserve copy being made of the data in the Administrations and the Environment. The back-up procedure used by Twinfield is as follows. Twinfield will make every effort to a) make an interim copy each hour, which will be kept for one day, b) make a reserve copy once a day that will be kept for 7 days, c) make a week backup each Friday that will be kept for 3 weeks, d) make a month backup each last day of the month that will be kept for one year, and e) keep the backup of 1st January of each year for 7 years. Each reserve copy will be compressed and encrypted via the Rijndael (AES) or 448- Blowfish encryption principle. The reserve copies are saved in an externally located data centre in a country forming part of the European Economic Area (EEA). Files in the function file management are not saved in the reserve copies. No reserve copies will be made of template Administrations.

21.2 After termination of the Subscription Agreement or an Administration and provided that the request thereto has been made in accordance with Articles 9.5 sub d or 9.6, Twinfield will, at the expense of Subscriber and provided that agreement has been reached by the Parties on the conditions thereof, make the audit file(s) of the relevant Administration(s) or specific data or records in the Environment or the relevant Administration(s) available to Subscriber, in a generally accessible file format. In case of such request Twinfield will make an offer to Subscriber as regards the data to be exported, the fee and the other terms and conditions of the data transfer. Such offer will be based on Twinfield's consultancy fees as specified in the Price List. Subscriber agrees that the liability of Twinfield for the availability, completeness, integrity or possibilities for use of such data is entirely excluded. Twinfield is in not obliged to convert the data provided or otherwise make them appropriate for use by Subscriber.

21.3 Subscriber can request the restoration of data using the reserve copies. To this end, a separate agreement must be made at the then applicable rate and under the then applicable terms and conditions.

Annex 3: AWS CUSTOMER AGREEMENT

Last updated March 15, 2012

(current AWS customers: See What's Changed)

This AWS Customer Agreement (this "**Agreement**") contains the terms and conditions that govern your access to and use of the Service Offerings (as defined below) and is an agreement between Amazon Web Services LLC ("**AWS**," "**we**," "**us**," or "**our**") and you or the entity you represent ("**you**"). This Agreement takes effect when you click an "I Accept" button or check box presented with these terms or, if earlier, when you use any of the Service Offerings (the "**Effective Date**"). You represent to us that you are lawfully able to enter into contracts (e.g., you are not a minor). If you are entering into this Agreement for an entity, such as the company you work for, you represent to us that you have legal authority to bind that entity. Please see Section 14 for definitions of certain capitalized terms used in this Agreement.

1. Use of the Service Offerings.

1.1 Generally. You may access and use the Service Offerings in accordance with this Agreement. Service Level Agreements may apply to certain Service Offerings. You will adhere to all laws, rules, and regulations applicable to your use of the Service Offerings, including the Service Terms, the Acceptable Use Policy and the other Policies as defined in Section 14.

1.2 Your Account. To access the Services, you must create an AWS account associated with a valid e-mail address. Unless explicitly permitted by the Service Terms, you may only create one account per email address. You are responsible for all activities that occur under your account, regardless of whether the activities are undertaken by you, your employees or a third party (including your contractors or agents) and, except to the extent caused by our breach of this Agreement, we and our affiliates are not responsible for unauthorized access to your account. You will contact us immediately if you believe an unauthorized third party may be using your account or if your account information is lost or stolen. You may terminate your account and this Agreement at any time in accordance with Section 7.

1.3 Support to You. If you would like support for the Services other than the support we generally provide to other users of the Services without charge, you may enroll for customer support in accordance with the terms of the AWS Premium Support Guidelines.

1.4 Third Party Content. Third Party Content, such as software applications provided by third parties, may be made available directly to you by other companies or individuals under separate terms and conditions, including separate fees and charges. Because we may not have tested or screened the Third Party Content, your use of any Third Party Content is at your sole risk.

2. Changes.

2.1 To the Service Offerings. We may change, discontinue, or deprecate any of the Service Offerings (including the Service Offerings as a whole) or change or remove features or functionality of the Service Offerings from time to time. We will notify you of any material change to or discontinuation of the Service Offerings.

2.2 To the APIs. We may change, discontinue or deprecate any APIs for the Services from time to time but will use commercially reasonable efforts to continue supporting the previous version of any API changed, discontinued, or deprecated for 12 months after the change, discontinuation, or deprecation (except if doing so (a) would pose a security or intellectual property issue, (b) is economically or technically burdensome, or (c) is needed to comply with the law or requests of governmental entities).

2.3 To the Service Level Agreements. We may change, discontinue or add Service Level Agreements from time to time.

3. Security and Data Privacy.

3.1 AWS Security. Without limiting Section 10 or your obligations under Section 4.2, we will implement reasonable and appropriate measures designed to help you secure Your Content against accidental or unlawful loss, access or disclosure.

3.2 Data Privacy. We participate in the safe harbor programs described in the Privacy Policy. You may specify the AWS regions in which Your Content will be stored and accessible by End Users. We will not move Your Content from your selected AWS regions without notifying you, unless required to comply with the law or requests of governmental entities. You consent to our collection, use and disclosure of information associated with the Service Offerings in accordance with our Privacy Policy, and to the processing of Your Content in, and the transfer of Your Content into, the AWS regions you select.

4. Your Responsibilities

4.1 Your Content. You are solely responsible for the development, content, operation, maintenance, and use of Your Content. For example, you are solely responsible for:

(a) the technical operation of Your Content, including ensuring that calls you make to any Service are compatible with then-current APIs for that Service;

(b) compliance of Your Content with the Acceptable Use Policy, the other Policies, and the law;

(c) any claims relating to Your Content; and

(d) properly handling and processing notices sent to you (or any of your affiliates) by any person claiming that Your Content violate such person's rights, including notices pursuant to the Digital Millennium Copyright Act.

4.2 Other Security and Backup. You are responsible for properly configuring and using the Service Offerings and taking your own steps to maintain appropriate security, protection and backup of Your Content, which may include the use of encryption technology to protect Your

Content from unauthorized access and routine archiving Your Content. AWS log-in credentials and private keys generated by the Services are for your internal use only and you may not sell, transfer or sublicense them to any other entity or person, except that you may disclose your private key to your agents and subcontractors performing work on your behalf.

4.3 End User Violations. You will be deemed to have taken any action that you permit, assist or facilitate any person or entity to take related to this Agreement, Your Content or use of the Service Offerings. You are responsible for End Users' use of Your Content and the Service Offerings. You will ensure that all End Users comply with your obligations under this Agreement and that the terms of your agreement with each End User are consistent with this Agreement. If you become aware of any violation of your obligations under this Agreement by an End User, you will immediately terminate such End User's access to Your Content and the Service Offerings.

4.4 End User Support. You are responsible for providing customer service (if any) to End Users. We do not provide any support or services to End Users unless we have a separate agreement with you or an End User obligating us to provide support or services.

5. Fees and Payment

5.1. Service Fees. We calculate and bill fees and charges monthly. We may bill you more frequently for fees accrued if we suspect that your account is fraudulent or at risk of non-payment. You will pay us the applicable fees and charges for use of the Service Offerings as described on the AWS Site using one of the payment methods we support. All amounts payable under this Agreement will be made without setoff or counterclaim, and without any deduction or withholding. Fees and charges for any new Service or new feature of a Service will be effective when we post updated fees and charges on the AWS Site unless we expressly state otherwise in a notice. We may increase or add new fees and charges for any existing Services by giving you at least 30 days' advance notice. We may charge you interest at the rate of 1.5% per month (or the highest rate permitted by law, if less) on all late payments.

5.2 Taxes. All fees and charges payable by you are exclusive of applicable taxes and duties, including VAT and applicable sales tax. You will provide us any information we reasonably request to determine whether we are obligated to collect VAT from you, including your VAT identification number. If you are legally entitled to an exemption from any sales, use, or similar transaction tax, you are responsible for providing us with legally-sufficient tax exemption certificates for each taxing jurisdiction. We will apply the tax exemption certificates to charges under your account occurring after the date we receive the tax exemption certificates. If any deduction or withholding is required by law, you will notify us and will pay us any additional amounts necessary to ensure that the net amount that we receive, after any deduction and withholding, equals the amount we would have received if no deduction or withholding had been required. Additionally, you will provide us with documentation showing that the withheld and deducted amounts have been paid to the relevant taxing authority.

6. Temporary Suspension

6.1 Generally. We may suspend your or any End User's right to access or use any portion or all of the Service Offerings immediately upon notice to you if we determine:

(a) your or an End User's use of or registration for the Service Offerings (i) poses a security risk to the Service Offerings or any third party, (ii) may adversely impact the Service Offerings or the systems or Content of any other AWS customer, (iii) may subject us, our affiliates, or any third party to liability, or (iv) may be fraudulent;

(b) you are, or any End User is, in breach of this Agreement, including if you are delinquent on your payment obligations for more than 15 days; or

(c) you have ceased to operate in the ordinary course, made an assignment for the benefit of creditors or similar disposition of your assets, or become the subject of any bankruptcy, reorganization, liquidation, dissolution or similar proceeding.

6.2 Effect of Suspension. If we suspend your right to access or use any portion or all of the Service Offerings:

(a) you remain responsible for all fees and charges you have incurred through the date of suspension;

(b) you remain responsible for any applicable fees and charges for any Service Offerings to which you continue to have access, as well as applicable data storage fees and charges, and fees and charges for in-process tasks completed after the date of suspension;

(c) you will not be entitled to any service credits under the Service Level Agreements for any period of suspension; and

(d) we will not erase any of Your Content as a result of your suspension, except as specified elsewhere in this Agreement.

Our right to suspend your or any End User's right to access or use the Service Offerings is in addition to our right to terminate this Agreement pursuant to Section 7.2.

7. Term; Termination

7.1. Term. The term of this Agreement will commence on the Effective Date and will remain in effect until terminated by you or us in accordance with Section 7.2.

7.2 Termination.

(a) Termination for Convenience. You may terminate this Agreement for any reason by (i) providing us notice and (ii) closing your account for all Services for which we provide an account closing mechanism. We may terminate this Agreement for any reason by providing you 30 days advance notice.

(b) Termination for Cause.

(i) By Either Party. Either party may terminate this Agreement for cause upon 30 days advance notice to the other party if there is any material default or breach of this Agreement by the other party, unless the defaulting party has cured the material default or breach within the 30 day notice period.

(ii) By Us. We may also terminate this Agreement immediately upon notice to you (A) for cause, if any act or omission by you or any End User results in a suspension described in Section 6.1, (B) if our relationship with a third party partner who provides software or other technology we use to provide the Service Offerings expires, terminates or requires us to change the way we provide the software or other technology as part of the Services, (c) if we believe providing the Services could create a substantial economic or technical burden or material security risk for us, (D) in order to comply with the law or requests of governmental entities, or (E) if we determine use of the Service Offerings by you or any End Users or our provision of any of the Services to you or any End Users has become impractical or unfeasible for any legal or regulatory reason.

7.3. Effect of Termination.

(a) Generally. Upon any termination of this Agreement:

(i) all your rights under this Agreement immediately terminate;

(ii) you remain responsible for all fees and charges you have incurred through the date of termination, including fees and charges for in-process tasks completed after the date of termination;

(iii) you will immediately return or, if instructed by us, destroy all AWS Content in your possession; and

(iv) Sections 4.1, 5.2, 7.3, 8 (except the license granted to you in Section 8.4), 9, 10, 11, 13 and 14 will continue to apply in accordance with their terms.

(b) Post-Termination Assistance. Unless we terminate your use of the Service Offerings pursuant to Section 7.2(b), during the 30 days following termination:

(i) we will not erase any of Your Content as a result of the termination;

(ii) you may retrieve Your Content from the Services only if you have paid any charges for any post-termination use of the Service Offerings and all other amounts due; and

(iii) we will provide you with the same post-termination data retrieval assistance that we generally make available to all customers.

Any additional post-termination assistance from us is subject to mutual agreement by you and us.

8. Proprietary Rights

8.1 Your Content. As between you and us, you or your licensors own all right, title, and interest in and to Your Content. Except as provided in this Section 8, we obtain no rights under this Agreement from you or your licensors to Your Content, including any related intellectual property rights. You consent to our use of Your Content to provide the Service Offerings to you and any End Users. We may disclose Your Content to provide the Service Offerings to you or any End Users or to comply with any request of a governmental or regulatory body (including subpoenas or court orders).

8.2 Your Submissions. Your Submissions will be governed by the terms of the Apache Software License, unless you specify one of our other supported licenses at the time you submit Your Submission.

8.3 Adequate Rights. You represent and warrant to us that: (a) you or your licensors own all right, title, and interest in and to Your Content and Your Submissions; (b) you have all rights in Your Content and Your Submissions necessary to grant the rights contemplated by this Agreement; and (c) none of Your Content, Your Submissions or End Users' use of Your Content, Your Submissions or the Services Offerings will violate the Acceptable Use Policy.

8.4 Service Offerings License. As between you and us, we or our affiliates or licensors own and reserve all right, title, and interest in and to the Service Offerings. We grant you a limited, revocable, non-exclusive, non-sublicensable, non-transferrable license to do the following during the Term: (i) access and use the Services solely in accordance with this Agreement; and (ii) copy and use the AWS Content solely in connection with your permitted use of the Services. Except as provided in this Section 8.4, you obtain no rights under this Agreement from us or our licensors to the Service Offerings, including any related intellectual property rights. Some AWS Content may be provided to you under a separate license, such as the Apache Software License or other open source license. In the event of a conflict between this Agreement and any separate license, the separate license will prevail with respect to that AWS Content.

8.5 License Restrictions. Neither you nor any End User may use the Service Offerings in any manner or for any purpose other than as expressly permitted by this Agreement. Neither you nor any End User may, or may attempt to, (a) modify, alter, tamper with, repair, or otherwise create derivative works of any software included in the Service Offerings (except to the extent software included in the Service Offerings are provided to you under a separate license that expressly permits the creation of derivative works), (b) reverse engineer, disassemble, or decompile the Service Offerings or apply any other process or procedure to derive the source code of any software included in the Service Offerings, (c) access or use the Service Offerings in a way intended to avoid incurring fees or exceeding usage limits or quotas, or (d) resell or sublicense the Service Offerings. All licenses granted to you in this Agreement are conditional on your continued compliance this Agreement, and will immediately and automatically terminate if you do not comply with any term or condition of this Agreement. During and after the Term, you will not assert, nor will you authorize, assist, or encourage any third party to assert, against us or any of our affiliates, customers, vendors, business partners, or licensors, any patent infringement or other intellectual property infringement claim regarding any Service Offerings you have used. You may only use the AWS Marks in accordance with the Trademark Use Guidelines.

8.6 Suggestions. If you provide any Suggestions to us or our affiliates, we will own all right, title, and interest in and to the Suggestions, even if you have designated the Suggestions as confidential. We and our affiliates will be entitled to use the Suggestions without restriction. You hereby irrevocably assign to us all right, title, and interest in and to the Suggestions and agree to provide us any assistance we may require to document, perfect, and maintain our rights in the Suggestions.

9. Indemnification.

9.1. General. You will defend, indemnify, and hold harmless us, our affiliates and licensors, and each of their respective employees, officers, directors, and representatives from and against any claims, damages, losses, liabilities, costs, and expenses (including reasonable attorneys' fees) arising out of or relating to any third party claim concerning: (a) your or any End Users' use of the Service Offerings (including any activities under your AWS account and use by your employees and personnel); (b) breach of this Agreement or violation of applicable law by you or any End User; (c) Your Content or the combination of Your Content with other applications, content or processes, including any claim involving alleged infringement or misappropriation of third-party rights by Your Content or by the use, development, design, production, advertising or marketing of Your Content; or (d) a dispute between you and any End User. If we or our affiliates are obligated to respond to a third party subpoena or other compulsory legal order or process described above, you will also reimburse us for reasonable attorneys' fees, as well as our employees' and contractors' time and materials spent responding to the third party subpoena or other compulsory legal order or process at our then-current hourly rates.

9.2. Process. We will promptly notify you of any claim subject to Section 9.1, but our failure to promptly notify you will only affect your obligations under Section 9.1 to the extent that our failure prejudices your ability to defend the claim. You may: (a) use counsel of your own choosing (subject to our written consent) to defend against any claim; and (b) settle the claim as you deem appropriate, provided that you obtain our prior written consent before entering into any settlement. We may also assume control of the defense and settlement of the claim at any time.

10. Disclaimers.

THE SERVICE OFFERINGS ARE PROVIDED "AS IS." WE AND OUR AFFILIATES AND LICENSORS MAKE NO REPRESENTATIONS OR WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE REGARDING THE SERVICE OFFERINGS OR THE THIRD PARTY CONTENT, INCLUDING ANY WARRANTY THAT THE SERVICE OFFERINGS OR THIRD PARTY CONTENT WILL BE UNINTERRUPTED, ERROR FREE OR FREE OF HARMFUL COMPONENTS, OR THAT ANY CONTENT, INCLUDING YOUR CONTENT OR THE THIRD PARTY CONTENT, WILL BE SECURE OR NOT OTHERWISE LOST OR DAMAGED. EXCEPT TO THE EXTENT PROHIBITED BY LAW, WE AND OUR AFFILIATES AND LICENSORS DISCLAIM ALL WARRANTIES, INCLUDING ANY IMPLIED WARRANTIES OF MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, OR QUIET ENJOYMENT, AND

ANY WARRANTIES ARISING OUT OF ANY COURSE OF DEALING OR USAGE OF TRADE.

11. Limitations of Liability.

WE AND OUR AFFILIATES OR LICENSORS WILL NOT BE LIABLE TO YOU FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL OR EXEMPLARY DAMAGES (INCLUDING DAMAGES FOR LOSS OF PROFITS, GOODWILL, USE, OR DATA), EVEN IF A PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. FURTHER, NEITHER WE NOR ANY OF OUR AFFILIATES OR LICENSORS WILL BE RESPONSIBLE FOR ANY COMPENSATION, REIMBURSEMENT, OR DAMAGES ARISING IN CONNECTION WITH: (A) YOUR INABILITY TO USE THE SERVICES, INCLUDING AS A RESULT OF ANY (I) TERMINATION OR SUSPENSION OF THIS AGREEMENT OR YOUR USE OF OR ACCESS TO THE SERVICE OFFERINGS, (II) OUR DISCONTINUATION OF ANY OR ALL OF THE SERVICE OFFERINGS, OR, (III) WITHOUT LIMITING ANY OBLIGATIONS UNDER THE SLAS, ANY UNANTICIPATED OR UNSCHEDULED DOWNTIME OF ALL OR A PORTION OF THE SERVICES FOR ANY REASON, INCLUDING AS A RESULT OF POWER OUTAGES, SYSTEM FAILURES OR OTHER INTERRUPTIONS; (B) THE COST OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; (c) ANY INVESTMENTS, EXPENDITURES, OR COMMITMENTS BY YOU IN CONNECTION WITH THIS AGREEMENT OR YOUR USE OF OR ACCESS TO THE SERVICE OFFERINGS; OR (D) ANY UNAUTHORIZED ACCESS TO, ALTERATION OF, OR THE DELETION, DESTRUCTION, DAMAGE, LOSS OR FAILURE TO STORE ANY OF YOUR CONTENT OR OTHER DATA. IN ANY CASE, OUR AND OUR AFFILIATES' AND LICENSORS' AGGREGATE LIABILITY UNDER THIS AGREEMENT WILL BE LIMITED TO THE AMOUNT YOU ACTUALLY PAY US UNDER THIS AGREEMENT FOR THE SERVICE THAT GAVE RISE TO THE CLAIM DURING THE 12 MONTHS PRECEDING THE CLAIM.

12. Modifications to the Agreement.

We may modify this Agreement (including any Policies) at any time by posting a revised version on the AWS Site or by otherwise notifying you in accordance with Section 13.7. The modified terms will become effective upon posting or, if we notify you by email, as stated in the email message. By continuing to use the Service Offerings after the effective date of any modifications to this Agreement, you agree to be bound by the modified terms. It is your responsibility to check the AWS Site regularly for modifications to this Agreement. We last modified this Agreement on the date listed at the beginning of this Agreement.

13. Miscellaneous.

13.1 Confidentiality and Publicity. You may use AWS Confidential information only in connection with your use of the Service Offerings as permitted under this Agreement. You will not disclose AWS Confidential Information during the Term or at any time during the 5 year period following the end of the Term. You will take all reasonable measures to avoid disclosure, dissemination or unauthorized use of AWS Confidential Information, including, at a minimum, those measures you take to protect your own confidential information of a similar

nature. You will not issue any press release or make any other public communication with respect to this Agreement or your use of the Service Offerings. You will not misrepresent or embellish the relationship between us and you (including by expressing or implying that we support, sponsor, endorse, or contribute to you or your business endeavors), or express or imply any relationship or affiliation between us and you or any other person or entity except as expressly permitted by this Agreement.

13.2 Force Majeure. We and our affiliates will not be liable for any delay or failure to perform any obligation under this Agreement where the delay or failure results from any cause beyond our reasonable control, including acts of God, labor disputes or other industrial disturbances, systemic electrical, telecommunications, or other utility failures, earthquake, storms or other elements of nature, blockages, embargoes, riots, acts or orders of government, acts of terrorism, or war.

13.3 Independent Contractors; Non-Exclusive Rights. We and you are independent contractors, and neither party, nor any of their respective affiliates, is an agent of the other for any purpose or has the authority to bind the other. Both parties reserve the right (a) to develop or have developed for it products, services, concepts, systems, or techniques that are similar to or compete with the products, services, concepts, systems, or techniques developed or contemplated by the other party and (b) to assist third party developers or systems integrators who may offer products or services which compete with the other party's products or services.

13.4 No Third Party Beneficiaries. This Agreement does not create any third party beneficiary rights in any individual or entity that is not a party to this Agreement.

13.5 U.S. Government Rights. The Service Offerings are provided to the U.S. Government as "commercial items," "commercial computer software," "commercial computer software documentation," and "technical data" with the same rights and restrictions generally applicable to the Service Offerings. If you are using the Service Offerings on behalf of the U.S. Government and these terms fail to meet the U.S. Government's needs or are inconsistent in any respect with federal law, you will immediately discontinue your use of the Service Offerings. The terms "commercial item" "commercial computer software," "commercial computer software documentation," and "technical data" are defined in the Federal Acquisition Regulation and the Defense Federal Acquisition Regulation Supplement.

13.6 Import and Export Compliance. In connection with this Agreement, each party will comply with all applicable import, re-import, export, and re-export control laws and regulations, including the Export Administration Regulations, the International Traffic in Arms Regulations, and country-specific economic sanctions programs implemented by the Office of Foreign Assets Control. For clarity, you are solely responsible for compliance related to the manner in which you choose to use the Service Offerings, including your transfer and processing of Your Content, the provision of Your Content to End Users, and the AWS region in which any of the foregoing occur.

13.7 Notice.

(a) To You. We may provide any notice to you under this Agreement by: (i) posting a notice on the AWS Site; or (ii) sending a message to the email address then associated with your

account. Notices we provide by posting on the AWS Site will be effective upon posting and notices we provide by email will be effective when we send the email. It is your responsibility to keep your email address current. You will be deemed to have received any email sent to the email address then associated with your account when we send the email, whether or not you actually receive the email.

(b) To Us. To give us notice under this Agreement, you must contact AWS as follows: (i) by facsimile transmission to 206-266-7010; or (ii) by personal delivery, overnight courier or registered or certified mail to Amazon Web Services LLC, 410 Terry Avenue North, Seattle, WA 98109-5210. We may update the facsimile number or address for notices to us by posting a notice on the AWS Site. Notices provided by personal delivery will be effective immediately. Notices provided by facsimile transmission or overnight courier will be effective one business day after they are sent. Notices provided registered or certified mail will be effective three business days after they are sent.

(c) Language. All communications and notices to be made or given pursuant to this Agreement must be in the English language.

13.8 Assignment. You will not assign this Agreement, or delegate or sublicense any of your rights under this Agreement, without our prior written consent. Any assignment or transfer in violation of this Section 13.8 will be void. Subject to the foregoing, this Agreement will be binding upon, and inure to the benefit of the parties and their respective successors and assigns.

13.9 No Waivers. The failure by us to enforce any provision of this Agreement will not constitute a present or future waiver of such provision nor limit our right to enforce such provision at a later time. All waivers by us must be in writing to be effective.

13.10 Severability. If any portion of this Agreement is held to be invalid or unenforceable, the remaining portions of this Agreement will remain in full force and effect. Any invalid or unenforceable portions will be interpreted to effect and intent of the original portion. If such construction is not possible, the invalid or unenforceable portion will be severed from this Agreement but the rest of the Agreement will remain in full force and effect.

13.11 Governing Law; Venue. The laws of the State of Washington, without reference to conflict of law rules, govern this Agreement and any dispute of any sort that might arise between you and us. Any dispute relating in any way to the Service Offerings or this Agreement where a party seeks aggregate relief of $7,500 or more will be adjudicated in any state or federal court in King County, Washington. You consent to exclusive jurisdiction and venue in those courts. We may seek injunctive or other relief in any state, federal, or national court of competent jurisdiction for any actual or alleged infringement of our, our affiliates, or any third party's intellectual property or other proprietary rights. The United Nations Convention for the International Sale of Goods does not apply to this Agreement.

13.12 Entire Agreement; English Language. This Agreement includes the Policies and is the entire agreement between you and us regarding the subject matter of this Agreement. This Agreement supersedes all prior or contemporaneous representations, understandings, agreements, or communications between you and us, whether written or verbal, regarding the

subject matter of this Agreement. Notwithstanding any other agreement between you and us, the security and data privacy provisions in Section 3 of this Agreement contain our and our affiliates' entire obligation regarding the security, privacy and confidentiality of Your Content. We will not be bound by, and specifically object to, any term, condition or other provision which is different from or in addition to the provisions of this Agreement (whether or not it would materially alter this Agreement) and which is submitted by you in any order, receipt, acceptance, confirmation, correspondence or other document. If the terms of this document are inconsistent with the terms contained in any Policy, the terms contained in this document will control, except that the Service Terms will control over this document. If we provide a translation of the English language version of this Agreement, the English language version of the Agreement will control if there is any conflict.

14. Definitions.

"Acceptable Use Policy" means the policy currently available at http://aws.amazon.com/aup, as it may be updated by us from time to time.

"API" means an application program interface.

"AWS Confidential Information" means all nonpublic information disclosed by us, our affiliates, business partners or our or their respective employees, contractors or agents that is designated as confidential or that, given the nature of the information or circumstances surrounding its disclosure, reasonably should be understood to be confidential. AWS Confidential Information includes: (a) nonpublic information relating to our or our affiliates or business partners' technology, customers, business plans, promotional and marketing activities, finances and other business affairs; (b) third-party information that we are obligated to keep confidential; and (c) the nature, content and existence of any discussions or negotiations between you and us or our affiliates. AWS Confidential Information does not include any information that: (i) is or becomes publicly available without breach of this Agreement; (ii) can be shown by documentation to have been known to you at the time of your receipt from us; (iii) is received from a third party who did not acquire or disclose the same by a wrongful or tortious act; or (iv) can be shown by documentation to have been independently developed by you without reference to the AWS Confidential Information.

"AWS Content" means Content we or any of its affiliates make available in connection with the Services or on the AWS Site to allow access to and use of the Services, including WSDLs; Documentation; sample code; software libraries; command line tools; and other related technology. AWS Content does not include the Services.

"AWS Marks" means any trademarks, service marks, service or trade names, logos, and other designations of AWS and its affiliates that we may make available to you in connection with this Agreement.

"AWS Premium Support Guidelines" means the guidelines currently available athttp://aws.amazon.com/premiumsupport/guidelines, as they may be updated by us from time to time.

"AWS Site" means http://aws.amazon.com and any successor or related site designated by us.

"Content" means software (including machine images), data, text, audio, video, images or other content.

"Documentation" means the developer guides, getting started guides, user guides, quick reference guides, and other technical and operations manuals and specifications for the Services located athttp://aws.amazon.com/documentation, as such documentation may be updated by us from time to time.

"End User" means any individual or entity that directly or indirectly through another user: (a) accesses or uses Your Content; or (b) otherwise accesses or uses the Service Offerings under your account. The term "End User" does not include individuals or entities when they are accessing or using the Services or any Content under their own AWS account, rather than your account.

"Notice and Procedure for Making Claims of Copyright Infringement" means the procedures currently located at http://aws.amazon.com/terms#notice-and-procedure-for-making-claims-of-copyright-infringement, as they may be updated by us from time to time.

"Policies" means the Acceptable Use Policy, the Site Terms, the Service Terms, the Trademark Use Guidelines, all restrictions described in the AWS Content and on the AWS Site, and any other policy or terms referenced in or incorporated into this Agreement. Policies does not include whitepapers or other marketing materials referenced on the AWS Site.

"Privacy Policy" means the privacy policy currently referenced at http://aws.amazon.com/privacy, as it may be updated by us from time to time.

"Service" means each of the web services made available by us or our affiliates, including those web services described in the Service Terms.

"Service Level Agreement" means all service level agreements that we offer with respect to the Services and post on the AWS Site, as they may be updated by us from time to time. The service level agreements we currently offer with respect to the Services are located at http://aws.amazon.com/ec2-sla/, http://aws.amazon.com/s3-sla/, and http://aws.amazon.com/cloudfront/sla.

"Service Offerings" means the Services (including associated APIs), the AWS Content, the AWS Marks, the AWS Site, and any other product or service provided by us under this Agreement. Service Offerings do not include Third Party Content.

"Service Terms" means the rights and restrictions for particular Services located athttp://aws.amazon.com/serviceterms, as they may be updated by us from time to time.

"Site Terms" means the terms of use located at http://aws.amazon.com/terms/, as they may be updated by us from time to time.

"Suggestions" means all suggested improvements to the Service Offerings that you provide to us.

"Term" means the term of this Agreement described in Section 7.1.

"Third Party Content" means Content made available to you by any third party on the AWS Site or in conjunction with the Services.

"Trademark Use Guidelines" means the guidelines and license located at http://aws.amazon.com/trademark-guidelines/, as they may be updated by us from time to time.

"Your Content" means Content you or any End User (a) run on the Services, (b) cause to interface with the Services, or (c) upload to the Services under your account or otherwise transfer, process, use or store in connection with your account.

"Your Submissions" means Content that you post or otherwise submit to developer forums, sample code repositories, public data repositories, or similar community-focused areas of the AWS Site or the Services.

Changes posted March 15, 2012

Billing Frequency (Section 5.1)
The following sentence has been added to Section 5.1: "We may bill you more frequently for fees accrued if we suspect that your account is fraudulent or at risk of non-payment."

Suspension for Fraud (Section 6.1)

March 15, 2012 version:
(a) your or an End User's use of or registration for the Service Offerings (i) poses a security risk to the Service Offerings or any third party, (ii) may adversely impact the Service Offerings or the systems or Content of any other AWS customer, (iii) may subject us, our affiliates, or any third party to liability, or (iv) may be fraudulent.

August 23, 2011 version:
(a) your or an End User's use of the Service Offerings (i) poses a security risk to the Service Offerings or any third party, (ii) may adversely impact the Service Offerings or the systems or Content of any other AWS customer, or (iii) may subject us, our affiliates, or any third party to liability.

Separate License Applicability (Section 8.4)
The following has been added to the end of Section 8.4: "…or other open source license. In the event of a conflict between this Agreement and any separate license, the separate license will prevail with respect to that AWS Content."

License Restrictions (Section 8.5)
The following has been added to Section 8.5: "...(d) resell or sublicense the Service Offerings."

Assignment (Section 13.8)
The following sentence has been added to Section 13.8: “Any assignment or transfer in violation of this Section 13.8 will be void.”

Annex 4: CLOUDEE TERMS AND CONDITIONS

By clicking the check box on the sign-up form you (Customer) agree to become bound by the Terms and Conditions of this agreement, to the exclusion of all other terms. Please read carefully this agreement before using Cloudee.eu and make sure you understand what they say.
DataCamp Limited is a company incorporated and registered in England and Wales with number 07489096 whose registered office is at London Canary Wharf 29th floor, One Canada Square, Canary Wharf, London, UK (Supplier). DataCamp Limited agrees to provide services described in the Order for the fees stated in the Order.

- 1.1 The initial service term of this agreement shall begin on the date the Customer accepted the terms of the agreement by clicking the check box, i.e. the date on which the Customer first order services from the Supplier (Effective Date), and shall continue indefinitely unless terminated in accordance with the terms of this agreement.
- 1.2 The Supplier agrees to provide services described in the order for the fees stated in the order.
- 1.3 The Customer agrees to pay the agreed price to the Supplier and to provide necessary assistance to the Supplier. The Customer represents and warrants to the Supplier that the information he, she or it has provided and will provide to the Supplier for purposes of establishing and maintaining the service is accurate. If the Customer is an individual, the Customer represents and warrants to the Supplier that he or she is at least 18 years of age.
- 1.4 The specification of the services governed by this agreement is described on the web pages describing the particular service the Customer has purchased based on the description as it stands on the Effective Date. The Supplier may modify products and services from time-to-time. Should the description of services change subsequent to the Effective Date, the Supplier has no obligation to modify services to reflect such a change.
- 1.5 The Customer acknowledges that all intellectual property rights in the service and any modification belong and shall belong to the Supplier, and the Customer shall have no rights in or to the service other than the right to use it in accordance with the terms of this agreement.
- 1.6 The Supplier reserves the right to make changes to these terms at any time. To the extent the Supplier is able, the Supplier will give the Customer advance notice of these changes. If these changes materially affect the Customer's ability to use services, the Customer may terminate this agreement within 30 days of such a change. Otherwise, the Customer's continued use of the service is the Customer's consent to be bound by the changes.
- 1.7 In the case of conflict or ambiguity between any provision contained in the body of this agreement and any provision contained on the Supplier's website, the provision in the body of this agreement shall take precedence.
- 1.8 Questions about the terms of this agreement will be answered at e-mail address support@cloudee.eu at phone number +44 (0) 20 3514 2399.

- 2.1 The Supplier shall provide for each customer the free service as a promo for testing for a maximum of 7 days.
- 2.2 The fee is payable in advance on the first day of each billing cycle. The Customer's billing cycle shall be monthly, beginning on the Effective Date. The Supplier may require payment for the first billing cycle before beginning service.
- 2.3 The Customer is fully responsible for the accuracy and completeness of all data (such as change in billing or mailing address, credit card expiration) and timely notification of changes of these details. The Supplier is not responsible for any misunderstanding resulting from failure to notify of these changes by the Customer.
- 2.4 The Supplier may increase its fees for services, if such a change notifies the customer at least thirty (30) days prior to the effective date of new fees. The Customer is entitled to terminate this Agreement with effect from the fee change. If the Customer does not give a notice of non-renewal, the Customer shall be deemed to have accepted the new fee.
- 2.5 The Customer doesn't have the right to hold back any payment from the Supplier in case of service or availability problems.
- 2.6 The Customer acknowledges that the amount of the fee for the service is based on the Customer's agreement to pay the fee for the entire initial service term, or renewal term, as applicable.

  If the Customer terminates the service before the expiration of this period, the Supplier agrees to refund proportion of the payment for unused services to the Customer.

  All charges are non-refundable unless expressly stated otherwise, or otherwise provided by applicable law.

- 2.7 If the Customer believes that there is an error in calculation of the fee, the Customer has the right claim settlement prices for the service.

- 3.1 The Supplier warrants that the service will conform in all material respects to the specification. If the Customer notifies the Supplier in writing of any defect or fault in the service in consequence of which it fails to conform in all material respects to the specification, and such defect or fault does not result from the Customer, or anyone acting with the authority of the Customer, having used the service outside the terms of this agreement, for a purpose or in a context other than the purpose or context for which it was designed, the Supplier shall, at the Supplier's option, do one of the following: a) replace the service; or b) repair the service; or c) terminate this agreement immediately by notice in writing to the Customer and refund any of the fee paid by the Customer as at the date of termination (less a reasonable sum in respect of the Customer's use of the service to date of termination), provided the Customer provides all the information that may be necessary to assist the Supplier in resolving the defect or fault.
- 3.2 The Supplier does not represent or warrant that the service will be error-free or accessible at all times, the delivery of the services will be uninterrupted or without delay, defects will be corrected. The Customer agrees that the Supplier shall not be responsible for unauthorized access to or alteration of the Customer's data. The Supplier disclaims any and all warranties regarding services provided by third parties, regardeless of whether those services appear to be provided by the Supplier.

- 3.3 The Customer represents and warrants to the Supplier that has the experience and knowledge necessary to use services and will provide the Supplier with material that may be implemented by the Supplier to provide services without extra effort on its part.
- 3.4 The Supplier shall have no liability for any losses or damages which may be suffered by the Customer (or any person claiming under or through the Customer), whether the same are suffered directly or indirectly or are immediate or consequential, and whether the same arise in contract, tort (including negligence) or otherwise howsoever, which fall within any of the following categories: a) special damage even though the Supplier was aware of the circumstances in which such special damage could arise; b) loss of profits; c) loss of business opportunity; d) loss of goodwill; e) loss of data.
- 3.5 The Customer agrees that, in entering into this agreement, either it did not rely on any representations (whether written or oral) of any kind or of any person other that those expressly set out in this agreement or (if it did rely on any representations, whether written or oral, not expressly set out in this agreement) that it shall have no remedy in respect of such representations and (in either case) the Supplier shall have no liability otherwise than pursuant to the express terms of this agreement.
- 3.6 Notwithstanding anything else in the agreement to the contrary, the maximum aggregate liability of the Supplier and any of its employees, agents or affiliates, under any theory of law (including breach of contract, tort, strict liability and infringement) shall be a payment of money not to exceed the amount payable by the Customer for 3 months of service.
- 3.7 No party shall be liable to the other for any delay or non-performance of its obligations under this agreement arising from any cause beyond its control (force majeure) including, without limitation, any of the following: act of God, governmental act, significant failure of a portion of the power grid, significant failure of the Internet, natural disaster, war, flood, explosion, riot, insurrection, epidemic, strikes or other organized labor action, terrorist activity, or other events of a magnitude or type for which precautions are not generally taken in the industry. For the avoidance of doubt, nothing in clause 3.7 shall excuse the Customer from any payment obligations under this agreement.
- 3.8 All other conditions, warranties or other terms which might have effect between the parties or be implied or incorporated into this agreement or any collateral contract, whether by statute, common law or otherwise, are hereby excluded, including, without limitation, the implied conditions, warranties or other terms as to satisfactory quality, fitness for purpose or the use of reasonable skill and care.

- 4.1 Either party may terminate this agreement at any time on written notice to the other if the other: a) is in material or persistent breach of any of the terms of this agreement and either that breach is incapable of remedy, or the other party fails to remedy that breach within 30 days after receiving written notice requiring it to remedy that breach; or b) is unable to pay its debts (within the meaning of section 123 of the Insolvency Act 1986), or becomes insolvent, or is subject to an order or a resolution for its liquidation, administration, winding-up or dissolution (otherwise than for the purposes of a solvent amalgamation or reconstruction), or has an administrative or other receiver, manager, trustee, liquidator, administrator or similar officer appointed over all or any substantial part of its assets, or enters into or proposes any composition or arrangement with its creditors generally, or is subject to any analogous event or proceeding in any applicable jurisdiction.

- 4.2 Notwithstanding clause 4.1, the Supplier may at any time terminate this agreement for any reason by giving written notice to the Customer, whereas the Customer may terminate this agreement by giving 7 days' notice in writing to the Supplier if it wishes to stop using the service.
- 4.3 The Customer agrees that the Supplier may suspend services to the Customer without notice and without liability if: a) the Supplier reasonably believes that the services are being used in violation of the this agreement; b) the Supplier reasonably believes that the suspension of service is necessary to protect its network or its other customers; c) as requested by a law enforcement or regulatory agency; or d) the Customer failures to pay fees due. The Customer shall pay the Supplier's reasonable reinstatement fee if service is reinstituted following a suspension of service under this subsection.
- 4.4 On termination for any reason: a) all rights granted to the Customer under this agreement shall cease; b) the Customer shall cease all activities authorised by this agreement; c) the Customer shall immediately pay to the Supplier any sums due to the Supplier under this agreement.

- 5.1 The Customer acknowledges that the Supplier processes personal data, as defined under the relevant data protection laws, of the users of the service for the purpose of complying with its obligations under this agreement.
- 5.2 The Customer hereby warrants that it has the consent of the users to disclose their personal data to the Supplier for the purpose of using the service and that for the same purpose the users have agreed that their personal data may be transferred to territories outside the EEA.
- 5.3 The Supplier will take all steps reasonably necessary to ensure that personal data is treated securely.
- 5.4 The Customer agrees that the Supplier may, without notice to the Customer, report to the appropriate authorities any conduct by the Customer or any of the Customer's customers or end users that the Supplier believes violates applicable law, and provide any information that it has about the Customer or any of its customers or end users in response to a formal or informal request from a law enforcement or regulatory agency or in response to a formal request in a civil action that on its face meets the requirements for such a request.
- 5.5 The Supplier shall not disclose any data to third parties, but may process such data in duly anonymised and aggregate form for purposes such as internal statistics, commercial sale and promotion.
- 5.6 Each party shall, during the term of this agreement and thereafter, keep confidential all, and shall not use for its own purposes (unless in accordance with clause 5.5) nor without the prior written consent of the other disclose to any third party, any information of a confidential nature (including, without limitation, trade secrets and information of commercial value) which may become known to such party from the other party and which relates to the other party, unless such information is public knowledge or already known to such party at the time of disclosure, or subsequently becomes public knowledge other than by breach of this agreement, or subsequently comes lawfully into the possession of such party from a third party. The provisions of this clause shall remain in full force and effect for 1 year after the termination of this agreement for any reason.

- 6.1 The Customer agree to indemnify, hold harmless and defend the Supplier from and against any and all claims, damages, losses, liabilities, suits, actions, demands, proceedings (whether legal or administrative), and expenses (including, but not limited to, reasonable attorney's fees) threatened, asserted, or filed by a third party against any of the indemnified parties arising out of or relating to the Customer's breach of any term or condition of this agreement, the Customer's use of the service, any violation by the Customer of any of the Supplier's policies, and/or any acts or omissions by the Customer. In such a case, the Supplier will provide the Customer with written notice of such claim, suit or action. The Customer shall cooperate as fully as reasonably required in the defense of any claim. The Supplier reserves the right, at its own expense, to assume the exclusive defense and control of any matter subject to indemnification by the Customer.

- 7.1 The Customer will not use the service in any way or for any purpose that would violate, or would have the effect of violating, any applicable laws, rules or regulations or any rights of any third parties, including without limitation, any law or right regarding any copyright, patent, trademark, trade secret, music, image, or other proprietary or property right, false advertising, unfair competition, defamation, invasion of privacy or rights of celebrity.

- 8.1 No forbearance or delay by either party in enforcing its rights shall prejudice or restrict the rights of that party, and no waiver of any such rights or of any breach of any contractual terms shall be deemed to be a waiver of any other right or of any later breach.

- 9.1 In the event that any of the terms of this agreement become or are declared to be illegal or otherwise unenforceable, such term(s) shall be null and void and shall be deemed deleted from this agreement. All remaining terms of this agreement shall remain in full force and effect. Notwithstanding the foregoing, if this paragraph becomes applicable and, as a result, the value of this agreement is materially impaired for either party, as determined by such party in its sole discretion, then the affected party may terminate this agreement by written notice to the other.

- 10.1 This agreement does not create any agency, partnership, joint venture, or franchise relationship. Neither party has the right or authority to, and shall not, assume or create any obligation of any nature whatsoever on behalf of the other party or bind the other party in any respect whatsoever.

- 11.1 No term of this agreement is intended to confer a benefit on, or to be enforceable by, any person who is not a party to this agreement.

- 12.1 Any notice required to be given pursuant to this agreement shall be in writing, and shall be sent to the other party by first-class mail or e-mail.

- 13.1 This agreement and the website www.cloudee.eu, in so far as it describes the specification, contain the whole agreement between the parties relating to the subject matter hereof and supersede all prior agreements, arrangements and understandings between the parties relating to that subject matter.

- 14.1 This agreement, its subject matter or its formation (including non-contractual disputes or claims) shall be governed by and construed in accordance with English law and submitted to the non-exclusive jurisdiction of the English courts.

Annex 5: MICROSOFT ONLINE SUBSCRIPTION AGREEMENT

This Microsoft Online Subscription Agreement is between the entity that accepts this agreement ("you") and Microsoft Corporation ("us", "we"). This agreement consists of: (1) the below terms and conditions; (2) the Online Services Use Rights; (3) the Service Level Agreements; and (4) the pricing and payment terms available via the Portal. This agreement is effective on the date we provide you with a confirmation for your first Order. You enter into this agreement for business purposes only.

Terms and Conditions

1.Definitions.

"Affiliate" means any legal entity that a party owns, that owns a party, or that is under common ownership with a party. "Ownership" means, for purposes of this definition, control of more than a 50% interest in an entity. If you are an agency of a state, provincial, or local government, "Affiliate" means (1) any government agency, department, office, instrumentality, division, unit or other entity, of your state, provincial or local government that you supervise or is part of you, or which supervises you or you are part of, or which is under common supervision with you; (2) any county, borough, commonwealth, city, municipality, town, township, special purpose district, or other similar type of governmental instrumentality established by the laws of your state or province and located within your state's or province's jurisdiction and geographic boundaries; and (3) any other entity in your state or province expressly authorized by the laws of your state or province to purchase under state or provincial contracts; provided that a state or province and its Affiliates shall not, for purposes of this definition, be considered to be Affiliates of the federal government or its Affiliates. Notwithstanding the forgoing, provincial Crown corporations are not Affiliates for the purposes of this definition. If you are an agency of the U.S. government, "Affiliate" means any other agency of the U.S. government. If you are an agency of the Canadian government, "Affiliate" means any other agency of the Canadian government, except for a federal Crown corporation.

"Committed Offering" means the Subscription option for a Product as described below in Section 3a.

"Communities" means one or more forums that we or an Affiliate of ours may establish for customers or the general public to obtain information or collaborate regarding the use of the Product(s), as may be accessible via the Portal or at an alternate website we identify.

"Consumption Offering" means the Subscription option for a Product as described below in Section 3a.

"Customer Data" means all data, including all text, sound, or image files that you provided, or are provided on your behalf, to us through your use of the Online Services.

"License" means the right to copy, install, use, access, display, run and/or otherwise interact with a Product, as applicable, and as may be further described in the Online Services Use Rights.

"Licensed Software" means any software product as available on the Portal. Licensed Sofware is offered on a standalone basis or as a component of an Online Service.

"Online Service" means any online service as available on the Portal. An Online Service may include Supplemental Software and/or Licensed Software.

"Online Services Use Rights" means the use rights for each Product published at http://www.microsoft.com/licensing/onlineuserights/english or at an alternate site that we identify.

"Order" means an order for a Product on the Portal. An Order may include multiple Subscriptions to a Product.

"Portal" means the Microsoft Online Services Portal at http://www.microsoft.com/online or at an alternate website we identify.

"Product" means any Online Service and any Licensed Software as described on the Portal.

"Service Level Agreement" means an agreement representing commitments we make regarding delivery and/or performance of an Online Service.

"Subscription" means the part of the Order identifying the specific Product being ordered and may include the quantity, ship-to address, or other information.

"Supplemental Software" means software provided to you as part of an Online Service and which is used with the Online Service to enable certain functions of the Online Service.

"Term" means the duration of a Subscription.

2.Your use of our Products.

a. General. This agreement governs your use of the Products. You may need to activate an Online Service prior to use. We grant you a License to Products you ordered provided you pay for them and comply with this agreement. Your License is non-exclusive, non-perpetual, and, unless specifically allowed, non-transferable. Minimum system requirements or other factors may affect your ability to use Products. We reserve all rights not expressly granted in this agreement.

b. Service Level Agreement. We will provide Online Services according to the Service Level Agreement(s) located athttp://www.microsoft.com/licensing/contracts or at an alternate site that we identify.

c. Privacy, Use and Security of Customer Data. We will handle your Customer Data according to the privacy, use and security terms set forth in the Online Services Use Rights.

d. Supplemental Software. To enable optimal access and use of certain Online Services, you may need to install Supplemental Software, including upgrades and/or updates. This agreement governs your use of Supplemental Software, and any upgrades/updates, unless we present separate license terms to you upon installation. Any separate license terms are between us and you, not your users. You may use Supplemental Software only to support the applicable Online Service. Copies you make must be complete copies (including copyright and trademark notices) and made from Microsoft-approved media or a network source. You may use a third party to make and install these copies, but you agree to be responsible for that third party's actions. You agree to use reasonable efforts to inform anyone you allow to use the Supplemental Software that it is licensed from us and subject to the terms of this agreement.

We may check the version of the Supplemental Software you are using and recommend or download updates, with or without notice, to your devices. Your right to use the Supplemental Software ends when your right to use the Online Service ends or when we update the Online Service and it no longer supports the Supplemental Software, whichever comes first. You must uninstall the Supplemental Software when your right to use it ends. We may also disable it at that time.

e. Licensed Software. We grant you Licenses for the number of copies of Licensed Software you ordered. We also grant you the right to use a prior (older) version in place of a Licensed Software version you license if we specify such use in the Online Services Use Rights.

(i) Qualifying desktop operating system License. Licenses for desktop operating system software available under this agreement are upgrade Licenses only ("OS Upgrade Licenses"), not full Licenses. All your computers that will run OS Upgrade Licenses must be licensed to run one of the full qualifying desktop operating systems identified in the Online Services Use Rights.

You may internally reassign OS Upgrade Licenses from the original computer to a replacement computer within your enterprise, so long as (1) the replacement computer is licensed to run a full qualifying operating system identified in the Online Services Use Rights, (2) you remove any OS Upgrade License software from the original computer, and (3) that reassignment is not within 90 days of the last reassignment.

(ii) When Licenses become perpetual. Unless you obtain perpetual Licenses under a buy-out option indicated on the Portal, a License to Licensed Software you obtained under this agreement lasts only for the Subscription Term. Any

references in the Online Services Use Rights to running Licensed Software on a perpetual basis apply only if you obtained perpetual Licenses.

(iii) License confirmation. Proof of your Licenses consists of: (1) this agreement, (2) any Order confirmation, (3) documentation evidencing License transfers (for any permitted transfers), and, if applicable, (4) proof of payment.

(iv) License rights are not related to fulfillment of software media. Your acquisition of software media does not affect your License to Licensed Software obtained under this agreement. We license Licensed Software to you, we do not sell it.

(v) Copies. You may make as many copies of the Licensed Software as you need to distribute them throughout your organization provided you have a valid License for each such copy. Copies you make must be complete copies (including copyright and trademark notices). You must make copies from Microsoft-approved media or a network source acquired from or made available by a Microsoft-approved fulfillment source. You may use a third party to make and install these copies, but you agree to be responsible for that third party's actions. You must use reasonable efforts to inform anyone you allow to use the Licensed Software that it is licensed from us and subject to the terms of this agreement.

(vi) Right to re-image. In certain cases, you may re-image a software product on a device by using the Licensed Software media. If you acquired the software product (1) from an original equipment manufacturer (OEM), (2) as a full packaged software product through a retail source, or (3) under another Microsoft program, you may use the media provided to you under this agreement to create images for use in place of copies provided through that separate source. You have this right provided that:

1) You have a valid license from the separate source for each copy of the software product that is re-imaged;

2) The Licensed Software, language, version, and components of the copies is identical to the software product, language, version, and all components of the copies they replace and the number of copies or instances of the re-imaged software product permitted remains the same;

3) Except for copies of an operating system and copies of software product licensed under another Microsoft program, the Licensed Software type (e.g., upgrade or full License) is identical to the software product type from the separate source;

4) You comply with any specific requirements for re-imaging identified in the Online Services Use Rights; and

5) You agree that re-images made under this subsection remain subject to the terms and use rights provided with the software product from the separate source.

This subsection does not create or extend any warranty or support obligation.

(vii) Transferring and assigning Licenses.

1) License Transfers. License transfers are not permitted, except as explicitly set forth in the Perpetual License Transfer Form. The resale of Licenses is prohibited, including any transfer by you or your Affiliate(s) for the purpose of transferring those Licenses to an unaffiliated third party.

2) Internal Assignment of Licenses. Licenses must be assigned to a single user or device. Licenses may be reassigned as described in the Online Services Use Rights.

f. Limitations on use. The Online Services Use Rights identify limitations on your use of Products in addition to those specified in this agreement. You may not reverse engineer, decompile or disassemble any Product, except where applicable law permits it despite this limitation. You may not rent, lease, lend, resell, or host to or for third parties any Product, except as expressly permitted for a given Product in the Online Services Use Rights. You may not separate and use the components of a Product on two or more computers, upgrade or downgrade components at different times, or transfer components separately, except as provided in the Online Services Use Rights.

g. Responsibility for your IDs and accounts. You are responsible for protecting the confidentiality of any Microsoft Live IDs and Microsoft Online Services IDs associated with this agreement. In addition, you are responsible for your passwords, if any, and all activity with your Online Service accounts including that of users you provision and dealings with third parties that take place through your account or associated accounts. You must keep your accounts and passwords confidential. You must tell us right away about any possible misuse of your accounts or any security incident related to the Online Service.

h. Your responsibility for use of Communities. You are responsible for your users' use of any Community, including ensuring compliance with the terms governing the Community located at the Community's website. We specifically disclaim any liability arising from or related to your or your users' use of or inability to use a Community's website.

3.Ordering, pricing, payments, renewals, and taxes.

a. The Portal provides the available Subscription options for each Product and they can generally be categorized as follows:

(i) Committed Offerings: You commit in advance to purchase a specific quantity of Products for use during a Term. You pay on a periodic basis during the Term in advance.

(ii) Consumption Offerings: You pay based on actual usage in the preceding month with no upfront commitment. Payment is on a periodic basis in arrears.

(iii) Combination Offerings: You may have a Subscription that is a combination of a Committed Offering and a Consumption Offering.

With respect to any offerings available free of charge, provisions in this agreement with respect to pricing, cancellation fees and payment do not apply.

b. Ordering. You can place an Order on the Portal.

(i) For Committed Offerings, you may increase or decrease the quantity of Product Licenses during the Term. Licenses added to a Subscription will expire at the end of the original Term. If you decrease the quantity during a Term, we may charge you a cancellation fee for the decrease in quantity as described below in the section titled "Cancellation of a Subscription." A Subscription for a Product that is supplemental requires a Subscription for the underlying Product. A Subscription for a supplemental Product may end when the Subscription for the underlying Product ends. Each Subscription shall be for a defined Term (e.g., 30 days or 12 months) as specified on the Portal.

(ii) You may place Orders for your Affiliates under this agreement and grant your Affiliates administrative rights to manage their Product. Affiliates may not place Orders under this agreement. If you grant any rights to your Affiliates, such Affiliates shall be bound by this agreement. You also may assign a third party a License to a Product if the third party needs such a License as part of your internal business needs. You agree to be jointly and severally liable for any Product ordered for or other actions taken by any of your Affiliates or any third party to which you provide rights under this agreement.

c. Prices. Pricing and payment terms for Products are available on or through the Portal. Payments are due and must be made according to the payment option you selected for each Product on the Portal.

(i) For Committed Offerings, the price level may be based on your Order quantity for a given Product. Your price level may be adjusted if the number of Licenses in the Subscription is increased or decreased during the Term and you qualify for a different price level. Price level changes are not retroactive. Any resulting change in the payment due for that Subscription will be pro-rated. Prices for each price level are fixed at the time the Order is first placed and shall apply throughout the Term. Prices and price levels are subject to change at the beginning of any Subscription renewal.

(ii) For Consumption Offerings, the pricing and rate schedules will be based on actual usage and subject to change at any time upon notice.

d. Subscription renewal.

(i) For Committed Offerings, you may choose to have a Subscription (1) automatically renew or (2) not renew upon expiration of the Term. You can change this selection at any time during the Term on the Portal. If you elect to have the Subscription automatically renew and the existing Term is longer than one calendar month, we will provide you with written notice of the automatic renewal prior to the expiration of the Term. If you elect to automatically renew a Subscription, the quantity of Licenses in each Subscription at the time of renewal, including any Licenses added during the Term, is automatically renewed.

(ii) For Consumption Offerings, renewal is unnecessary because your ability to use the Product will continue until the applicable Product is discontinued.

(iii) Trial Subscriptions cannot be renewed.

e. New agreement. Before you place new Orders or renew any Subscriptions, we may require you to enter into an updated agreement that will govern your new Orders and renewal Subscriptions from that date forward.

f. Taxes. Any amounts owed to us are exclusive of any taxes. You shall pay any applicable value added, goods and services, sales, or like taxes that are owed with respect to any Order placed under the agreement and which we are permitted to collect from you under applicable law. You shall be responsible for any applicable stamp taxes and for all other taxes that you are legally obligated to pay including any taxes that arise on the distribution or provision of Products to your Affiliates. We shall be responsible for all taxes based upon our net income or on our property ownership. If any taxes are required to be withheld on payments you make to us, you may deduct such taxes from the amount owed to us and pay them to the appropriate taxing authority, provided however that you promptly secure and deliver an official receipt for those withholdings and other documents we reasonably request to claim a foreign tax credit or refund. You will make certain that any taxes withheld are minimized to the extent possible under applicable law.

4.Term, suspension, and termination.

a. Agreement term and termination. This agreement will remain in effect unless you terminate it subject to the terms of this Section. For Committed Offerings, termination will only terminate your right to renew Subscriptions under an existing Order or place new Orders for additional Products under this agreement. Termination will not affect any Subscription not otherwise terminated and this agreement shall remain in effect for such Subscription for the remainder of the

Term. For Consumption Offerings, termination will end Customer's right to use the Product.

b. Termination of a Subscription. You may terminate a Subscription at any time during its Term. A termination will be effective at the end of the monthly Subscription cycle during which you terminate the Subscription. You must pay for the period prior to the termination effective date.

For Committed Offerings the following applies:

(i) One month ("month-to-month") Subscription. A one month Subscription may be terminated anytime without any fee.

(ii) One year Subscription (including prepaid). If you terminate a one year Subscription within 30 days of the date on which the Subscription became effective or was renewed, you must pay for the initial 30 days of the Subscription. No payments will be due for the remainder of the Subscription. If you terminate a Subscription at any other time during the Term, you must pay 25% of the Subscription fee otherwise due for the remainder of the one year Term.

c. How to terminate the agreement or a Subscription. You must follow the process, if available, on the Portal or otherwise contact Microsoft customer service (see contact information on the Portal) to terminate the agreement or a Subscription.

d. Effect of termination or expiration on Licensed Software. If the agreement or a Subscription is terminated or expires, and you do not exercise an available buy-out option, then you must delete all copies of Supplemental Software and Licensed Software licensed under this agreement and destroy any associated media. We may ask you to provide written certification of the deletion and destruction.

e. Expiration or termination: Customer Data. Upon expiration or termination of each Subscription, you must tell us whether to:

(i) retain Customer Data in your paid account upon conversion from a trial account; or

(ii) disable your account and then delete your Customer Data; or

(iii) retain your Customer Data in a limited function account for at least 90 days after expiration or termination of your Subscription (the "retention period") so that you may extract your Customer Data.

1) If you indicate (ii), you will not be able to extract your Customer Data from your account. If you indicate (iii), you will be able to extract your Customer Data via our standard processes and tools, and you will reimburse us if

there are any applicable costs. If you do not indicate (ii) or (iii), we will retain your Customer Data in accordance with (iii).

2) Following the expiration of the retention period, we will disable your account and then delete your Customer Data.

You agree that, other than as described above, we have no obligation to continue to hold, export or return your Customer Data. You agree that we have no liability whatsoever for deletion of your Customer Data pursuant to these terms.

f. Regulatory environment: modification or termination. We may modify or terminate an Online Service in any country where there is any current or future government requirement or obligation that subjects us to any regulation or requirement not generally applicable to businesses operating there, presents a hardship for us to continue operating the Online Service without modification, and/or causes us to believe these terms or the Online Service may be in conflict with any such requirement or obligation. For example, we may modify or terminate the Online Service in connection with a government requirement that would cause us to be regulated as a telecommunications provider.

5.Confidentiality.

You agree that you shall treat the design and performance of the Online Services that are accessible to you only via password protected access and any documentation or materials we make available to you under this agreement as confidential and shall not disclose them to any third party except in the furtherance of the parties' business relationship with each other. If you are a government customer, this Section is subject to the requirements of applicable trade secret, public records, and similar laws. Neither party shall make any public statement concerning the terms or our business relationship as provided in this agreement without the other party's prior written consent.

6.Warranties.

a. Limited warranty. We warrant that:

(i) Online Services will perform in accordance with the Service Level Agreement; and

(ii) Licensed Software will perform substantially as described in the applicable Microsoft user documentation.

b. Limited warranty term. The limited warranty for:

(i) Online Services is for the duration of your use of the Online Service; and

(ii) Licensed Software is one year from the date you first use it.

c. Limited warranty exclusions. This limited warranty is subject to the following limitations:

(i) any implied warranties, guarantees or conditions not able to be disclaimed as a matter of law will last one year from the start of the limited warranty;

(ii) this limited warranty does not cover problems caused by accident, abuse or use of the Products in a manner inconsistent with this agreement or the Online Services Use Rights, or resulting from events beyond our reasonable control;

(iii) this limited warranty does not apply to problems caused by the failure to meet minimum system requirements; and

(iv) this limited warranty does not apply to free, trial, pre-release or beta Products.

d. Remedies for breach of limited warranty. If we fail to meet any of the above limited warranties and you notify us within the warranty period that a Product does not meet the limited warranty, then we will:

(i) for Online Services, provide the remedies identified in the Service Level Agreement for the affected Online Service; and

(ii) for Licensed Software, at our option either (1) return the price paid or (2) repair or replace the Licensed Software.

These are your only remedies for breach of the limited warranty, unless other remedies are required to be provided under applicable law.

e. DISCLAIMER OF OTHER WARRANTIES. OTHER THAN THIS LIMITED WARRANTY, WE PROVIDE NO OTHER EXPRESS OR IMPLIED WARRANTIES OR CONDITIONS. WE DISCLAIM ANY IMPLIED REPRESENTATIONS, WARRANTIES OR CONDITIONS, INCLUDING WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, SATISFACTORY QUALITY, TITLE OR NON-INFRINGEMENT. THESE DISCLAIMERS WILL APPLY UNLESS APPLICABLE LAW DOES NOT PERMIT THEM.

7.Defense of infringement, misappropriation, and third party claims.

a. Our agreement to protect. We will defend you against any claims made by an unaffiliated third party that any Product infringes that party's patent, copyright or trademark or makes intentional unlawful use of its trade secret. We will also pay the amount of any resulting adverse final judgment (or settlement to which we consent). This Section provides your exclusive remedy for these claims.

b. Limitations on defense obligation. Our obligations will not apply to the extent that the claim or award is based on:

(i) Customer Data, code, or materials you provided as part of the use of an Online Service;

(ii) your use of the Product after we notify you to discontinue that use due to a third party claim;

(iii) your combination of the Product with a non-Microsoft product, data or business process;

(iv) damages attributable to the value of the use of a non-Microsoft product, data or business process;

(v) modifications you make to the Product;

(vi) your redistribution of the Product to, or use for the benefit of, any unaffiliated third party;

(vii) your use of Microsoft's trademark(s) without express written consent to do so; or

(viii) any trade secret claim, where you acquire the trade secret or undisclosed information (1) through improper means; (2) under circumstances giving rise to a duty to maintain its secrecy or limit its use; or (3) from a person (other than us or one of our Affiliates) who owed to the party asserting the claim a duty to maintain the secrecy or limit the use of the trade secret.

You will reimburse us for any costs or damages that result from any of the above actions.

c. Specific rights and remedies in case of infringement.

(i) Our rights in addressing possible infringement. If we receive information concerning an infringement claim related to a Product, we may, at our expense and without obligation to do so: (1) procure for you the right to continue to use the allegedly infringing Product; (2) modify the Product; (3) replace the Product with a functional equivalent, to make it non-infringing, in which case you will immediately stop using the allegedly infringing Product after receiving notice from us; or (4) terminate any applicable Subscriptions if the Product was provided free of charge.

(ii) Your specific remedy in case of injunction. If, as a result of an infringement claim, your use of a Product is enjoined by a court of competent jurisdiction, we will, at our option, either: (1) procure the right to continue its use; (2) replace it with a functional equivalent; (3) modify it to make it non-infringing; (4) terminate the License for the infringing Product and refund any amounts you paid in advance for unused Product; or (5) terminate any applicable Subscriptions if the Product was provided free of charge.

d. Your agreement to protect. You will defend us and our Affiliates against any claims made by an unaffiliated third party (1) that any Customer Data or non-Microsoft software we host on your behalf infringes the third party's patent, copyright, or trademark or makes intentional unlawful use of its Trade Secret, or (2) related to your use of the Product in violation of this agreement. You must pay the amount of any resulting adverse final judgment (or settlement to which you consent). This section provides our exclusive remedy for these claims.

e. Obligations of protected party. You must notify us promptly in writing of a claim subject to the subsection titled "Our agreement to protect" and we must notify you promptly in writing of a claim subject to the subsection titled "Your agreement to protect." The party invoking its right to protection must (1) give the other party sole control over the defense or settlement; and (2) provide reasonable assistance in defending the claim. The party providing the protection will reimburse the other party for reasonable out of pocket expenses that it incurs in providing assistance.

8.Limitation of liability.

a. Limitation on liability. Except as otherwise provided in this Section, to the extent permitted by applicable law, our and our Affiliates' and contractors' liability to you arising under this agreement is limited to direct damages up to the amount you paid us for the Product giving rise to that liability during the (1) Term or (2) twelve months prior to the filing of the claim, whichever is less. In the case of Products provided free of charge, or any code that you are authorized to redistribute to third parties without separate payment to Microsoft, our and our Affiliates' and contractors' liability to you arising under this agreement is limited to five United States dollars ($5.00 USD). These limitations apply regardless of whether the liability is based on breach of contract, tort (including negligence), strict liability, breach of warranties, or any other legal theory. However, these monetary limitations will not apply to:

(i) Our obligations under the Section titled "Defense of infringement, misappropriation, and third party claims";

(ii) liability for damages awarded by a court of final adjudication for our or our employees' or agents' gross negligence or willful misconduct;

(iii) liabilities arising out of any breach of our obligations under the Section entitled "Confidentiality", except that our and our Affiliates' and contractors' liability arising out of or in relation to Customer Data shall in all cases be limited to the amount you paid for the Online Service giving rise to that liability during the (1) Term or (2) twelve months prior to the filing of the claim, whichever is less; and

(iv) liability for personal injury or death caused by our negligence or that of our employees or agents or for fraudulent misrepresentation.

b. EXCLUSION OF CERTAIN DAMAGES. TO THE EXTENT PERMITTED BY APPLICABLE LAW, WHATEVER THE LEGAL BASIS FOR THE CLAIM, NEITHER PARTY, NOR ANY OF ITS AFFILIATES OR SUPPLIERS, WILL BE LIABLE FOR ANY INDIRECT, CONSEQUENTIAL, SPECIAL OR INCIDENTAL DAMAGES, DAMAGES FOR LOST PROFITS OR REVENUES, BUSINESS INTERRUPTION, OR LOSS OF BUSINESS INFORMATION ARISING IN CONNECTION WITH THIS AGREEMENT, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR IF SUCH POSSIBILITY WAS REASONABLY FORESEEABLE. HOWEVER, THIS EXCLUSION DOES NOT APPLY TO EITHER PARTY'S LIABILITY TO THE OTHER FOR VIOLATION OF ITS CONFIDENTIALITY OBLIGATIONS (EXCEPT TO THE EXTENT THAT SUCH VIOLATION RELATES TO CUSTOMER DATA), THE OTHER PARTY'S INTELLECTUAL PROPERTY RIGHTS, OR THE PARTIES' RESPECTIVE OBLIGATIONS IN THE SECTION TITLED "DEFENSE OF INFRINGEMENT, MISAPPROPRIATION, AND THIRD PARTY CLAIMS."

9.Verifying compliance.

During the Term of any Subscription and for three years thereafter, you must keep all usual and proper records relating to the Subscription(s) and your use of Products under this agreement. We may request that you conduct an internal audit of all Products in use throughout your organization, comparing the number of Licenses in use to the number of Licenses issued to and/or paid for by you. By requesting an audit, we do not waive our rights to enforce this agreement or to protect Microsoft intellectual property by any other means permitted by law.

If verification or self-audit reveals any unlicensed use, you must promptly order sufficient Licenses to cover your past and present use. If material unlicensed use is found, you must reimburse us for the costs we incurred in verification and acquire the necessary additional Licenses at retail license cost within 30 days.

10.Miscellaneous.

a. Notices to us. You must send notices, authorizations, and requests in connection with this agreement by regular or overnight mail, express courier, or fax to the addresses listed below. We will treat notices as delivered on the date shown on the return receipt or on the courier or fax confirmation of delivery.

Notices should be sent to:	Copies should be sent to:
Microsoft Corporation Volume Licensing Group One Microsoft Way Redmond, WA 98052 USA Via Facsimile: (425) 936-7329	Microsoft Corporation Legal and Corporate Affairs Volume Licensing Group One Microsoft Way Redmond, WA 98052 USA Via Facsimile: (425) 936-7329

b. Electronic notices to you. We may provide you with information about the Online Service in electronic form. It may be via email to the address you provide when you sign up for the Online Service (as you may update via the Portal) or through a web site that we identify. Notice via email is given as of the transmission date. As long as you use the Online Service, you have the software and hardware needed to receive these notices. You may not use the Online Service if you do not agree to receive these electronic notices. In addition, various service communications may be sent via email to account administrators you identify and may update via the Portal.

c. Assignment. You may not assign this agreement. We may assign this agreement to our Affiliates.

d. Severability. If a court holds any provision(s) of this agreement to be illegal, invalid or unenforceable, the rest of the document will remain in effect and this agreement will be amended to give effect to the eliminated provision to the maximum extent possible.

e. Waiver. A waiver of any breach of this agreement is not a waiver of any other breach. Any waiver must be in writing and signed by an authorized representative of the waiving party.

f. Applicable law. This agreement is governed by the laws of the State of Washington without regard to its conflict of laws principles, except that (1) if you are a U.S. Government entity, this agreement is governed by the laws of the United States, and (2) if you are a state or local government entity in the United States, this agreement is governed by the laws of that state. The 1980 United Nations Convention on Contracts for the International Sale of Goods and its related instruments will not apply to this agreement. The Products are protected by copyright and other intellectual property rights laws and international treaties.

g. Dispute resolution. Any action to enforce this agreement must be brought in the State of Washington, USA. This choice of jurisdiction does not prevent either party from seeking injunctive relief with respect to a violation of intellectual property rights or confidentiality obligations in any appropriate jurisdiction. If you are a

U.S. Government or state or local government entity, this Section does not apply and jurisdiction and venue will be determined by applicable law.

h. This agreement is not exclusive. You are free to enter into agreements to license, use or promote non-Microsoft software or services.

i. Entire agreement. This agreement constitutes the entire agreement concerning the subject matter and supersedes any prior or contemporaneous communications.

j. Survival. Provisions regarding fees, Online Services Use Rights, restrictions on use, transfer of Licenses, export restrictions, defense of infringement, misappropriation, and third party claims, limitations of liability, confidentiality, compliance verification, obligations on termination and the provisions in this Section entitled "Miscellaneous" will survive termination or expiration of this agreement.

k. Customer consent to partner fees. When you place an Order for certain Products, you may identify a "Partner of Record" associated with your Subscriptions. By identifying a Partner of Record, directly or by authorizing a third party to do so, you consent to us paying certain fees to the Partner of Record. The fees are for pre-sales support and may also include post-sales support. The fees are based on, and increase with the size of, your Order. Your prices for Products are the same whether or not you identify a Partner of Record.

l. No transfer of ownership. We do not transfer any ownership rights in any Products. We reserve all rights not specifically granted in this agreement. Products are protected by copyright and other intellectual property rights laws and international treaties.

m. Force majeure. Neither party will be liable for any failure in performance due to causes beyond either party's reasonable control (such as fire, explosion, power blackout, earthquake, flood, severe storms, strike, embargo, labor disputes, acts of civil or military authority, war, terrorism (including cyber terrorism), acts of God, acts or omissions of Internet traffic carriers, actions or omissions of regulatory or governmental bodies (including the passage of laws or regulations or other acts of government that impact the delivery of Online Services)). This Section will not, however, apply to your payment obligations under this agreement.

n. U.S. export jurisdiction. The Products are subject to U.S. export jurisdiction. You must comply with all applicable laws including the U.S. Export Administration Regulations, the International Traffic in Arms Regulations, as well as end-user, end-use and destination restrictions issued by U.S. and other governments. For additional information, see http://www.microsoft.com/exporting/.

o. Natural disaster. In the event of a natural disaster, we may post information or provide additional assistance or rights onhttp://www.microsoft.com.

Annex 6: CLOUDCONTROL – TERMS OF SERVICE

Last revised on May 20th, 2011

1. Your Agreement with cloudControl

1. Your use of the cloudControl's service is governed by this agreement (the "Terms"). "cloudControl" means cloudControl UG, located at Rudolf-Breitscheid-Str. 34, 14482 Potsdam, Germany. The "Services" means the services cloudControl makes available through the website, including our website, our cloud computing platform, our API, our Add-ons, and any other software or services by cloudControl in connection to any of those. Conflicting or deviating terms and conditions of purchase or other limitations of the user will not be recognized and are expressly excluded.
2. Subsidiary arrangements, assurances and other agreements, as well as alterations and additions to the Terms must be performed in written form in order to be effective.

2. Conclusion of the Agreement

1. By signing the agreement or registering an account the user makes an offer to cloudControl to sign and enter the contract. After receipt of the offer by cloudControl the user is bound to his offer for one week.
2. The contract is entered into effect if cloudControl accepts the offer within this period either in written agreement or by execution of the Service.
3. Offers from cloudControl are always subject to change and of non-binding nature. cloudControl may make the conclusion of a contract dependent upon the submission of written proof of authority, advance payment or a certificate of guarantee from a German bank.

3. Termination of the Service

The contract may be terminated at any time without prior notice or reason by ending the use and deleting the data.

4. cloudControl's Obligations

1. Contingent on cloudControl's acceptance of your offer, and subject to these Terms of

   Service, cloudControl agrees to provide the Services and to grant access to a running development and hosting platform. This covers, in particular – however non-exclusive – access to disk space, computing power and bandwidth. cloudControl's platform enables the customer to independently develop and operate software. The customer can expand the platform to his needs with the help of Add-ons. Add-ons are offered both by cloudControl itself and third party vendors. The scope of Service of the platform and single Add-ons depend on the product's description at the time of the order being placed.

2. If cloudControl offers free additional services which are not included in the Terms, cloudControl reserves the right to terminate those additional services at any time. No claim to a reduction or compensation will result from this discontinuation.

3. cloudControl is entitled to change, reduce or complete the range of Services stated in the Terms or to cancel the access to single Services. The user has to be informed about it in time.

5. Your Obligations

1. It is the user's obligation to use cloudControl's Services appropriately. The user is, in particular, obliged to,
   1. immediately inform cloudControl on changes to the contractual basis;
   2. not abuse the access to cloudControl's Services and to refrain from illegal or unlawful actions in any form. In particular it is prohibited for the user to use the Services of other users without their permission; not abuse Services agreed on in the contract between cloudControl and the client; not extract / read / change the content or passwords / E-Mails, files or similar from other users of cloudControl's Services or the system operator; unlawfully spread applications or software under license using cloudControl's platform; not interrupt or block communication services, e.g. causing overloads or distributing SPAM; spread or enable access to illegal content of any kind via cloudControl. This applies to pornographic, racist, violent or any otherwise illegal or immoral content, especially if it attacks the free democratic basic order or the concept of international understanding, as well as to propaganda material of anti-constitutional groups / parties and their replacement organizations and the provisioning of pornographic material related to child abuse. If a user fails to comply, he is required to compensate cloudControl for any

personal or objective expenditures or expenses caused by his behavior.

3. secure the fulfillment of all legal regulation and licensing requirements, as well as taking care that licensed permits are issued, as far as they will be necessary for taking part in the Services now an in the future;
4. comply with applicable data privacy laws and data security regulations;
5. notify cloudControl about any experienced deficiencies or damages (error notification) and to follow all actions enabling an identification of the deficiencies or damages and their cause or facilitate or quicken the elimination of the error;
6. after notification of the error to compensate cloudControl, if an investigation proves that the failure was caused by the user (and out of scope of the Terms and Services offered by cloudControl) himself or the cause was within his field of responsibility;

2. If the user does not oblige to the duties stated in paragraph 1 b) and 1 c), cloudControl is entitled to block and terminate the contract immediately or in any other cases after a failed warning.

6. Add-ons

1. cloudControl may make additional services ("Add-ons") available that extend the platform's functionality. Add-ons provided by third party providers are merely mediated between the provider and the customer. The customer acknowledges that by using third party Add-ons an agreement between the respective Add-on provider and the customer will be created and the terms of this Add-on provider apply. The Add-on Provider of each Add-on is solely responsible for that Add-on, the content therein, and any claims that you or any other party may have relating to that Add-on or your use of that Add-on.
2. The customer acknowledges that and agrees that cloudControl may reserve the right to submit claims in the name of the third party Add-on provider. The customer grants cloudControl the necessary rights to provide the third-party Add-on provider with the data required according to engage a contractual agreement with them.

7. Third Party Usage

1. The direct or indirect usage of cloudControl's Services by third parties is allowed. The user is allowed to use and resell cloudControl's Services. The user is obliged to correctly instruct third parties to cloudControl's Services. The user is responsible for the compliance of the Terms by the third party in the same way as he is responsible towards the

compliance of the Terms towards cloudControl himself.

2. The user is responsible for paying the fees that arose due to the third party usage of cloudControl's Services under his access and usage. The same applies for unauthorized use of Services by those third parties, unless the user proves that the unauthorized use was gained by circumventing or suspension of cloudControl's security mechanisms and he is not responsible for it.

8. Fees

1. The usage of the Services provided by cloudControl is free of charge within certain limits specified and set by cloudControl. There are both soft and hard limits. If the user crosses a soft limit he will receive a note from cloudControl via e-mail and is given the time to react to that e-mail. If the user crosses a hard limit, cloudControl has the rights to terminate the Services and to inform the visitor of the users application with an error message (503 Service Not Available) about the termination of the Services. The user is able to buy further resources (Boxes and Add-ons) as he wishes.
2. If not stated otherwise, cloudControl will charge the user for the Services agreed upon under the current fees or resp. tariffs and conditions. Prices stated include the respectively applicable VAT. The payable fees are billed monthly at the beginning of the subsequent month. All invoices are payable immediately, and must be made without deduction.
3. Boxes and Add-ons are charged per started hour. Calculations are based upon usage and consumption measured solely by cloudControl.

9. Right to Withhold, Right of Retention, Service Breakdown

1. The user only has set-off rights against claims by cloudControl, provided his counterclaim has been established legally or is undisputed or acknowledged. The user has the right of retention only for counter claims concerning Services covered by the contractual relationship.
2. Damage claims charged for delivery or service breakdown are excluded if cloudControl is not responsible for the breakdowns due to willful misconduct or gross negligence.
3. Usage or consumption based Services will not be charged during a period of considerable interferences. Asides that, the user is not entitled to any other reductions. A considerable interference is when
    1. the user cannot access the cloudControl platform or its Services for reasons that

are neither in control of the user nor third parties and

2. the use of the Services is generally much more difficult and/or the use of single Services listed in the Terms is impossible or limited.

4. In case of failures of Services due to faults which lie beyond the responsibility of cloudControl, a reduction is excluded. The same applies for the breakdown of Services due to necessary business interruption according to paragraph 11 within the Terms.

10. Delay of payment

1. Late payments may bear interest at the rate of 5 % (over the base rate permitted by law) per annum. If cloudControl is able to prove a higher damage by delayed payment, cloudControl is permitted to claim it.
2. cloudControl may terminate the contract without notice or claim the right of withdraw to its burden of Services, in particular the usage of domains, the connection of servers to the network or the interruption of the users connection, if the user is late with his payments at least for one month and cloudControl reminded and informed the user about possible consequences of the termination of the agreement and the right of withdraw.
3. The assertion of other claims is reserved to cloudControl.

11. Service Level Agreement

The availability of cloudControl's platform and cloudControl's own operated Add-ons is at least 99,95 % of the annual mean. Necessary downtime for preventive maintenance will be announced as early as possible and whenever possible at times with the lowest possible use. cloudControl will dispose of disruptions of its technical facilities – within the technical and operational capabilities of cloudControl – as quickly as possible.

12. License from cloudControl and Restrictions

1. cloudControl gives you a personal, worldwide, royalty-free, non-assignable and non-exclusive license to use the software provided to you by cloudControl as part of the Services as provided to you by cloudControl. This license is for the sole purpose of enabling you to use and enjoy the benefit of the Services provided by cloudControl, in the manner permitted by those Terms.
2. The user is explicitly prohibited from doing the following to the software as a whole or to parts of it:

1. copy, modify, create a derivative work of, reverse engineer, decompile or otherwise attempt to extract the source code of the Services or any part thereof, unless this is expressly permitted or required by law, or unless you have been specifically told that you may do so by cloudControl, in writing (e.g., through an open source software license); or
2. attempt to disable or circumvent any security mechanisms used by the Services or any application.

3. cloudControl hereby grants you a limited, non-exclusive, royalty-free, non-transferable license, with no right to sub-license, to display the cloudControl trademarks, limited to the blip and name mark description, for the sole purpose of promoting or advertising that you use the Services. When using the cloudControl marks you are bound to adhere to the guidelines. The customer agrees to his best knowledge use cloudControl's marks only in beneficial manners for cloudControl.

13. License from You

1. cloudControl claims no ownership or control over any content, data or application of its users. You retain all rights and obligations, and you are solely responsible for protecting those rights. Furthermore, by creating an Application through use of the Services, you give cloudControl a worldwide, royalty-free, and non-exclusive license to reproduce, adapt, modify, translate, publish, publicly perform, publicly display and distribute such Application for the sole purpose of enabling cloudControl to provide you with the Services.

2. You agree that cloudControl, in its sole discretion, may use your trade names, trademarks, service marks, logos, domain names and other distinctive brand features in presentations, marketing materials, customer lists, financial reports and Web site listings (including links to your website) for the purpose of advertising or publicizing your use of the Service.

14. Copyright Policy and Privacy

1. According to § 33, Sec. 1 of the German Data Security Law, the user is hereby informed that cloudControl is digitally processing personal data for tasks arising from the agreement.

2. If cloudControl employs Third Parties to perform those tasks, cloudControl is entitled to disclose the users data in strict adherence to § 28, German Data Security Law. Moreover, cloudControl is entitled to transmitting this data in cases where the detection, isolation and resolution of faults and failures in the system of cloudControl or in the system of Third Party providers depend on the data.
3. cloudControl affirms that cloudControl's employees, who act under these Terms, have been committed to the data confidentiality agreement according to § 5, German Data Security Law, and that cloudControl has taken the necessary technical and organizational measures to ensure the implementation of the regulations of the German Data Security Law according to § 9, German Data Security Law.

15. Limitation of Liabilities

1. cloudControl is liable for defects of quality and defects of title under the legal requirements. If only merchants are involved in the contract, $ 377 ff., German Commercial Code (HGB), applies. As applicable, the regulations of $ 44a, New Telecommunications Act (TKG), remain unaffected.
2. The liability for damage and legal responsibility of cloudControl is limited to intent and negligence, despite the liability for defects of quality and defects of title. cloudControl is also liable for slight negligence of major contractual obligations (obligations, whose infringement endangers the fulfillment of the agreement) and for the infringement of cardinal obligations (obligations, whose fulfillment itself first enable the proper enforcement of the agreement), but only for the predictable, agreement-typical damage. cloudControl is not liable for any other slight negligence of other obligations.
3. The limitations of liability according to section 2. are not applicable for the damage of life, body or health, for defects after adoption of a guarantee for the nature of the product or for fraudulent concealed defects. Liability according to the Product Liability Act (German: Produkthaftungsgesetz) remains unchanged.
4. If the liability of cloudControl is limited or excluded, it is also limited or excluded for the personal liability of its employees, representatives and agents.
5. The user is liable for any detrimental effects and disadvantages arising for cloudControl or Third Parties due to misuse or illegal use of cloudControl's Services or the violation of the user's obligations by the user himself.

16. General Legal Terms / Other Content

1. Place of performance is cloudControl's registered office in Potsdam, Germany.

2. Contracts concluded by these General Terms and Conditions are subject to German law to the exclusion of the UN Convention on Contracts for the International Sales of Goods.
3. For fully-qualified traders, cloudControl’s registered head office is the place of jurisdiction for all disputes arising from this contractual relationship. Similarly, this applies to legal persons under public law or public law special funds. cloudControl is also entitled to sue at the user's place of performance.
4. Should one or more individual parts of this contract be or become null and void, invalid or contestable entirely or partly, the validity of the remaining contract shall remain unaffected. The provisions thus rendered null or invalid shall in that case be interpreted or replaced by legal provisions under German law in a manner which ensures that the legal and economic purposes intended with the invalid provisions are achieved to the greatest extent possible. Analogously, the same shall apply to loopholes in need of supplementation, if any.

This is a translation of the cloudControl’s German terms of service. In any case of doubt the

German original version supersedes the English one.

Annex 7: CLOUDSIGMA – TERMS OF SERVICE

IMPORTANT LEGAL NOTICE

All services provided to you ("**you**", "**your**", "**user**") by CloudSigma ("**we**", "**us**", "**our**") apply to and are governed by these Terms of Service, the Acceptable Use Policy, the Privacy Policy, the Copyright Notice, the Service Level Agreement and the terms of your Purchase including any services provided through the Website and to any email, written or other correspondence relating to such services.

We retain the right and entitlement to revise or vary the Agreement and such revisions and variations will become binding on you as referred to below. The Agreement forms a legally binding agreement between us and you. Continued use of the Website or accepting Services offered by us by ticking the box 'Please confirm you have read and agree to our Terms of Service.' constitutes acceptance of the Agreement and formation of a legally binding agreement.

Any individual submitting a Purchase on behalf of a company or other legal entity represents and warrants that he or she has the legal authority and entitlement to bind that entity into the Agreement in which case "you", "your" and "user" shall mean the company or legal entity. The Agreement is the complete and exclusive agreement between you and us regarding its subject matter and supersedes and replaces any prior agreement, understanding, or communication, written or oral. If you do not accept any element of the Agreement you must not take up any of the Services offered by the Website. The Agreement imposes significant legal obligations on you and also places limits on your legal rights. Please seek independent legal advice before entering into the Agreement.

Any Purchase or commencement of supply of Services is done so on the basis that you have agreed to be legally bound to the terms of the Agreement and that you represent and warrant that you have the legal authority to enter into said Agreement.

The Services and Website are provided and offered for adults over the age of 18 only. If you are under 18 and/or you are not able to form legally binding contracts you should not use the Services and/or Website. You must check with the owner and/or providers of your internet access you are using in relation to the Services and/or Website that such access is lawful and allowed by any policy and/or terms of service governing the use of any equipment or internet connection.

By continuing to use the Website and any of the services offered by it, you are confirming that you are 18 or over and are accessing and using the Website and the services offered via the Website lawfully.

Variation to the Agreement

We reserve the right and entitlement to alter the Agreement at any time. We will notify you in accordance with the Agreement at least thirty (30) days prior to any alterations becoming valid and binding. Upon receipt of such notice, you will have the option either to terminate your account under the provisions of clause 10 and receive a refund for any positive account balance or to continue to use our Services and be bound by the altered Agreement. After the altered Agreement has come into force, purchase of additional Services or continued use of the Website including API usage constitutes your agreement to be legally bound to the altered Agreement's terms and conditions in full.

1.Definitions

In this Terms of Service:

- "**Acceptable Use Policy**" or "**AUP**" means the CloudSigma Acceptable Use Policy as of the date you make each Purchase or exchange of Credits for Services, as it may be amended in accordance with the Agreement.
- "**Agreement**" refers collectively to the Purchase, these Terms of Service, the Privacy Policy, the Copyright Notice, the Service Level Agreement and the Acceptable Use Policy.
- "**Agreement Date**" means the earlier of: (i) the date on which you accept these Terms of Service via the Website and/or (ii) the date you first use the Services including the purchase of Credits.
- "**API**" means CloudSigma's proprietary application programming interface.
- "**Beta Testing**" refers to a situation when you choose to participate in any beta test of a Service that is pre-release.
- "**CloudSigma**" means CLOUDSIGMA AG a Swiss company incorporated in the Canton of Zürich, Switzerland with incorporation number CH-020.3.034.422-0 and with registered address Sägereistrasse 35, CH-8152 Glattbrugg, Switzerland.
- "**Confidential Information**" means all non-public information disclosed by one party to the other at any time irrespective of the date of the Agreement, that the receiving party should reasonably understand to be confidential, including: (i) for you, all information stored or transmitted to or from the CloudSigma network, (ii) for us, any data centre or server designs, unpublished prices, unpublished terms of service, internal reports (including for auditing and security purposes), future company development plans, and any other proprietary information, and (iii) for both of us, any information marked as confidential. Confidential Information excludes any information or technology that is developed by one of us without reference to the other's Confidential Information or becomes available without violation of an applicable law or this Agreement.
- "**Copyright Notice**" means the CloudSigma Copyright Notice as of the date you make each Purchase or exchange of Credits for Services, as it may be amended in accordance with the Agreement.

- "**Credits**" means the non-refundable credits you Purchased via the Web Console which can be used in exchange for Services only. The credits are expressed in Swiss Francs (CHF), British Pounds (GBP), Euros (EUR) or United States Dollars (USD) on a one credit equals one currency unit basis. Credits are only expressed in relation to one currency equivalent in accordance with your currency selection upon opening an account with CloudSigma.
- "**Credit Balance**" means the number of Credits you have purchased less the number of credits exchanged in respect of Services provided in accordance with the Agreement.
- "**Junk Mail**" means email that is designated by our email systems as such as well as email reported by other users of CloudSigma and by you as unsolicited.
- "**Purchase**" means the purchase of Credit that you submit to us via the Website or any other written purchase provided to you by ourselves for signature which describes the Services you are purchasing and that is signed by you whether that be manually or electronically.
- "**Privacy Policy**" means the CloudSigma Privacy Policy as of the date you make each Purchase or exchange of Credits for Services, as it may be amended in accordance the Agreement.
- "**Service Level Agreement**" means the CloudSigma Service Level Agreement as of the date you make each Purchase or exchange of Credits for Services, as it may be amended in accordance with the Agreement.
- "**Services**" means services provided in exchange for Credit balance or provided free by CloudSigma as described on the pages of the Website relevant to that service. Services include only those services which are offered via the Website including but not limited to the provision of virtual servers, core-CPU power, disk data storage, RAM, network data transfer, IP addresses and VLANs. Services are provided in accordance with the Agreement.
- "**Web Console**" means the web console available at https://cs.cloudsigma.com which forms part of the Website and which you use to purchase Credits and to manage the provision of Services.
- "**Website**" means any website with a domain name ending "cloudsigma.com".
- "**Working Day**" means 9:00 a.m. – 5:00 p.m. Monday to Friday, Central European Time excluding Swiss national holidays.

2.Purchase of Credits

- **2.1** You acknowledge and agree that any Purchase made via the Website is for Credits that can be exchanged only in relation to Services. No amounts received by CloudSigma or Credits granted to you in relation to any Purchase (except under the terms of termination as set out in clause 10 of these Terms of Service) are:
  - **2.1.1** refundable;
  - **2.1.2** exchangeable for cash or any other form of payment; or
  - **2.1.3** useable in any manner other than in exchange for Services.
- **2.2** All Purchases must be made via:
  - **2.2.1** credit or debit card made via the Web Console; and

    - **2.2.2** bank transfer to the correct bank account matching the currency used for your account and using your unique bank transfer ID as available via the payment section of the Web Console.
- **2.3** Invoices are issued by us following shortly after any Purchase as we deem appropriate and necessary, and are also made available to you via the Web Console.
- **2.4** You acknowledge and accept that Services and/or continued access to the Web Console may be suspended or terminated immediately if any payment in relation to a Purchase is declined, delayed or refused by your financial institution and/or credit card or debit card provider.
- **2.5** We will adjust your Credit Balance in line with Services provided to you from time to time in accordance with the rates for exchange for those Services as advertised on our Website.
- **2.6** At our reasonable discretion if at any time during the Agreement you fail to meet an appropriate standard of creditworthiness, as determined at our sole discretion, we may either:
    - **2.6.1** require you to make advance Purchase(s) on a regular basis as we deem necessary;
    - **2.6.2** require you to make payments in relation to Purchase(s) by bank transfer that you could otherwise make under these Terms of Service by credit or debit card;
    - **2.6.3** impose a limit on the number of Credits you may Purchase; or
    - **2.6.4** impose restrictions or conditions on your right to use Services as we deem appropriate.
- **2.7** All Purchases must be made in the default currency of your account as selected by you upon account opening. Currency selection for your account is permanent. Accounts can be opened in Swiss Francs (CHF), British Pounds (GBP), Euros (EUR) or United States Dollars (USD).
- **2.8** The rates of exchange of Credits for Services will only be available to you in the default currency of your account. You may open multiple accounts with different default currencies.
- **2.9** In the event that any payment made by you in relation to a Purchase fails to be honoured or accepted by your financial institution and/or our Website's automated payment gateway then we reserve the right to charge a returned payment fee to cover any additional administration costs and/or any other associated costs which we may incur.
- **2.10** We reserve the right, at our absolute discretion, to suspend or cancel access to the Web Console, the API or to withhold the provision of any Services until payment in full of such amounts has been received by us including any fees we may have the right to charge you to return an unhonoured payment.
- **2.11** Upon termination of the Agreement your Credit Balance (unused or otherwise) that you have purchased will not be refunded or returned to you other than as specifically outlined under the terms of termination as set out in clause 10 of these Terms of Service.
- **2.12** We may charge interest on any overdue amounts at 1.5% per month (or the maximum legal rate if it is less than 1.5%). If any amount is overdue by more than twenty (20) Working Days and we bring legal action to collect or engage a collection agency to do so on our behalf, you must also pay our reasonable costs of collection, including but not limited to legal fees and court costs. All fees in relation to this are stated and will be charged in Swiss Francs (CHF).

3.Services

- **3.1** Contingent on CloudSigma's acceptance of your Purchase, and subject to these Terms of Service, CloudSigma agrees to provide Services in exchange for Credits at the rates of exchange outlined on the Website and Web Console.
- **3.2** We reserve the right to vary the rates of exchange of Credits for Services at any time at our sole discretion with immediate effect. Amended rates become applicable upon your next Purchase or exchange of Credits for Services.
- **3.3** Services offered via the Website may vary in scope and nature over time. You acknowledge, accept and agree that elements of the Services may be varied, updated, replaced, removed, supplemented or added to over time as we so determine appropriate.
- **3.4** We provide certain Services on a pre-paid subscription basis for the periods of 1 month, 3 months, 6 months and 1 year. Services purchased on a subscription basis are paid for in advance with Credits. Rates of exchange of Credits for Services are as outlined on the Website and Web Console. The number of Credits exchanged for Services is fixed at the time of the exchange for the period of the subscription in relation to the Services exchanged for credits at that time only.
- **3.5** We provide certain Services on a pay-as-you-go basis based on five minute billing cycles. We provide dynamic rates of exchange of Credits for Services which are updated every five minutes and are available via our Website and the Web Console. The number of Credits exchanged for Services on a pay-as-you-go basis is fixed at the time of the exchange for the period of the next five minute billing cycle.
- **3.6** Upon expiry of Services purchased on a pre-paid subscription basis you will automatically continue to be charged for the same Services on a pay-as-you-go basis at the on-going rates of exchange of Credits for Services at that time unless you cease to utilise our Services in relation to your expired subscription.
- **3.7** We shall provide the Service to you subject to the Agreement from the Agreement Date until the Service is fully delivered, its term expires, it is terminated or it is suspended under the terms of the Agreement.
- **3.8** The provision of Services is strictly subject to you maintaining a sufficient Credit Balance and you acknowledge, accept and agree that we may suspend or terminate Services to you if you have Credit Balance for less than 24 hours usage at your latest Service usage level and pay-as-you-go Service rates of exchange of Credits at that time.
- **3.9** We retain the right to verify your identity at any time. In the event that we are unable to verify your identity using reasonable endeavours, at our sole discretion we may require you to provide further proof of identity including but not limited to:
    - **3.9.1** an original or certified copy of photographic ID in the form of a driving licence or passport; and/or
    - **3.9.2** an original or certified copy of proof of address as deemed acceptable to us.
- **3.10** If you fail or are unwilling to provide such evidence as reasonably requested by us then we shall be entitled to immediately suspend and/or terminate your use of Services.
- **3.11** We shall not be responsible for any back up, recovery or other step required to ensure that data and information stored on the CloudSigma network and infrastructure as part of

provision of Services to you is recoverable in the case of any data loss, system fault, software failure, hardware failure or other activity which results in any loss of data, information or other item that is being stored as part of our Services.

- **3.12** We may suspend your Services without liability if:
  - **3.12.1** we have reason to believe that that the Services, have, are being or will be used in violation of the Agreement;
  - **3.12.2** you don't co-operate with reasonable investigations into suspected violations of the Agreement;
  - **3.12.3** we reasonably believe that your Services are being access or used by third parties without your authorisation;
  - **3.12.4** your Credit Balance is zero and/or insufficient to cover current Services being utilised by you;
  - **3.12.5** we reasonably believe it is necessary in order to protect our network infrastructure and Services to other customers;
  - **3.12.6** we discover that you are affiliated with a person or legal entity that has used our Services in the past and had their account terminated; or
  - **3.12.7** we are required to do so by law.
- **3.13** We will endeavour to provide you with reasonable notice of any suspension under this clause unless it our reasonable belief that an immediate suspension or shorter notice is required to protect our network infrastructure and services to other customers from significant operational or security risk or because we are compelled to do so by law.
- **3.14** We may continue to charge you for Services during any suspension resulting from a breach of obligations under the Agreement by you. You may be charged a reinstatement fee of up to CHF 100 to remove a suspension over your account.
- **3.15** We are not responsible for any unauthorized access to your data or the unauthorized use of Services under your account. You represent and warrant that you are solely responsible for the use of Services whether or not authorised by you, by any employee of yours, any person to whom you have given access to the Services and/or any person who gains access to your data or Services as a result of a failure by you to use reasonable security precautions. You hereby indemnify us and hold us harmless against all costs, claims, expenses and damages whatsoever arising from the use of or access to your data or Services by any third party.
- **3.16** We do not support any operating systems and/or other software which you run within your virtual servers as part of the Services we offer to you.
- **3.17** We do not monitor and have no liability for the contents of, any communications transmitted by you by virtue of our provision of the Services.
- **3.18** We have no obligation to provide security other than as stated in the Agreement. We disclaim any and all warranties not expressly stated in the Agreement, including the implied warranties of merchantability, fitness for a particular purpose, and non-infringement.
- **3.19** Both free Services and Services provided in exchange for Credits are provided to you on an AS IS basis.
- **3.20** We will be the sole arbiter of any dispute regarding the provision of Services and our decision will be final and binding.

4.Use of Services

- **4.1** You acknowledge, accept and agree to the following:
  - **4.1.1** only to use the Services in accordance with the Acceptable Use Policy;
  - **4.1.2** to comply with applicable laws at all times;
  - **4.1.3** not to interfere with Services or the provision of Services;
  - **4.1.4** you will at all times act in good faith in relation to the Services;
  - **4.1.5** not to continue to use Services if you have had an account suspended or terminated now or at any time in the past;
  - **4.1.6** that you are solely responsible for the suitability of the service chosen;
  - **4.1.7** to use reasonable security precautions in relation to your use of the Services;
  - **4.1.8** only share your password with a person or persons whom you have authorised to use your account;
  - **4.1.9** that your account is non-transferable and you will be liable for any and all activities undertaken using your user account together with the associated password, whether or not the person undertaking the activities has been authorised by you;
  - **4.1.10** keep up to date your billing, contact and other account information;
  - **4.1.11** that there are inherent risks with Internet connectivity that may result in the loss of your privacy, Confidential Information and/or property;
  - **4.1.12** immediately notify us of any suspected or actual unauthorised use of your account or any security breach; and
  - **4.1.13** to be solely and entirely responsible for maintaining at least one current backup copy outside of CloudSigma's network of all data (including but not limited to operating systems, content and programs) stored on CloudSigma's network to ensure that the potential for losses is mitigated.
- **4.2** You accept, acknowledge and agree that the Services may not be used in any situation where failure or fault of the Services could lead to death or serious bodily injury of any person, or to physical or environmental damage. This includes but is not limited to use of the Services in connection with modes of human mass transportation, nuclear and chemical facilities, critical infrastructure and medical devices whose failure or malfunction could result in harm to persons. Accordingly, without prejudice to any other disclaimer or limitation of liability in these Terms of Service, we specifically disclaim any express or implied warranty of fitness of the Service for use for such activities.
- **4.3** You accept and agree that you have no right to physical access to the premises from which the Service is provided without our explicit prior permission which will be granted at our sole discretion.
- **4.4** You may access the Services via our API in addition to via the Web Console. We reserve the right to change the API or suspend provision of the API at any time without notice.
- **4.5** You acknowledge, accept and agree that the provision of Services and the Website is strictly subject to:
  - **4.5.1** payment of all fees and charges in a prompt and timely manner;
  - **4.5.2** your full compliance with the Agreement including these Terms of Service;
  - **4.5.3** compliance with all relevant laws and regulations at all times; and
  - **4.5.4** maintenance of sufficient Credit Balance to ensure Services remain fully paid up;
  - **4.5.5** your purchasing of additional Credits as required via the Web Console once your Credit Balance becomes insufficient to maintain Services for 24 hours based on your

Service usage and pay-as-you-go rates of exchange of Credits for Services level at that time.

- **4.6** You represent and warrant to us that:
  - **4.6.1** you are 18 years of age or over, capable of taking responsibility for your own actions and of sound mind;
  - **4.6.2** you are able to enter into a legally binding agreement with us;
  - **4.6.3** if you are entering into the Agreement on behalf of a company or other legal entity you have the legal authority and entitlement to bind that entity into the Agreement;
  - **4.6.4** you are the person whose details are provided in connection with your user account;
  - **4.6.5** you are not an undischarged bankrupt or in a voluntary arrangement with your creditors; and
  - **4.6.6** you are not a person to whom CloudSigma is legally prohibited to provide Services.
- **4.7** Notwithstanding the provisions of clause 5 you shall effect and maintain sufficient insurance cover in respect of any case of damage, loss or claim in relation to data loss, system fault, software failure, hardware failure or other activity which results in any loss of data, information or other item that is being stored as part of our Services.
- **4.8** In the event that Services or access to the Website are suspended and/or terminated in relation to you and you believe that such action has been taken incorrectly, you must immediately contact us to allow a full investigation into the matter thereby limiting and mitigating against damage, loss and claims as a result of the suspension and/or termination.

5.Service Level Agreement

- **5.1** The Service Level Agreement forms part of the Agreement for Services you Purchase from CloudSigma.
- **5.2** Any credit resulting from the terms and conditions of the Service Level Agreement shall be credited to the Credit Balance for use against future Services. No credits resulting from the Service Level Agreement will be paid to you as cash or another form of refund.

6.Beta Services

A Service in Beta Testing is subject to the following terms:

- **6.1** You acknowledge the Beta Testing involves using a pre-release version that may not function properly;
- **6.2** You acknowledge that by Beta Testing you may expose yourself to higher than normal risks of operational failures;

- **6.3** The full commercial release version of the Beta Testing service may change substantially from the pre-release version. This may result in programs, networks and operations that ran on the Beta Testing pre-release version not working with the initial full commercial release or subsequent versions;
- **6.4** You are not entitled to any compensation under the Service Level Agreement for downtime, performance degradation, loss or corruption of data or any other problems that may result from your Beta Testing;
- **6.5** You agree to provide information and feedback on your Beta Testing in a form reasonably requested by us;
- **6.6** You agree that we may use your information and feedback for any purposes including but not limited to product development. We may use comments publicly for press and promotional materials with your prior permission;
- **6.7** You agree that any intellectual property inherent in your feedback or product development of our Services arising from your Beta Testing of any Service shall be owned exclusively by CloudSigma;
- **6.8** You agree that any information regarding your Beta Testing including your experiences and opinions are Confidential Information of CloudSigma, as defined in these Terms of Service. All information in relation to Beta Testing may only be used for the purpose of providing feedback to CloudSigma;
- **6.9** You should not use Beta testing for a live production environment. Beta Testing must not be used for critical computing functions including but not limited to any hazardous environments, life support or weapons systems;
- **6.10** Beta Testing is provided "AS IS" with no warranty whatsoever;
- **6.11** To the extent permitted by applicable law, CloudSigma disclaims any and all warranties with respect to Beta Testing including the implied warranties of merchantability, fitness for purpose and non-infringement;
- **6.12** The maximum aggregate liability of CloudSigma and any of its employees, agents, affiliates, or suppliers, under any theory of law for harm to you arising from your Beta Testing shall be a payment of money not to exceed One Hundred Swiss Francs (CHF 100.00); and
- **6.13** We reserve the exclusive right to terminate Beta Testing of a Service at any time at our sole discretion.

7.Support

- **7.1** In relation to a fault or disruption with our Services, we will use reasonable endeavours to respond to all requests.
- **7.2** We will use reasonable endeavours to resolve faults referred to us in accordance with clause 7.1.
- **7.3** All requests for support should be made to us using the support contact details provided on the Website.
- **7.4** We will provide you with reasonable notice for all schedule maintenance and/or downtime in advance and shall be entitled to undertake said scheduled maintenance and/or downtime.

- **7.5** In the event that it is our reasonable commercial believe that emergency maintenance and/or downtime is required, we may do so at any time without the requirement to provide reasonable notice to you.

8.Links to Third Party Web sites

- **8.1** Links to third party websites on the Website are provided from time to time solely for your convenience. If you use these links, you leave the Website.
- **8.2** We have not reviewed all of these third party websites and do not control and are not responsible for these websites or their content or availability.
- **8.3** We do not endorse or make any representations about them, or any material found there, or any results that may be obtained from using them.
- **8.4** If you decide to access any of the third party websites linked to the Website, you do so entirely at your own risk.
- **8.5** You acknowledge and agree that we will not be responsible for the availability of such third party websites and will not be responsible or liable for any content or services available from such third party websites. You should check the privacy statements and terms and conditions of use of third party websites accessible from the Website.

9.Links to the Website

- **9.1** If you would like to link to the Website, you may only do so subject to the following conditions:
  - **9.1.1** you do not remove, distort or otherwise alter the size or appearance of the "CloudSigma" logos or trademarks;
  - **9.1.2** you do not create a frame or any other browser or border environment around the Website;
  - **9.1.3** you do not in any way imply that we are endorsing any products or services other than our own;
  - **9.1.4** you do not misrepresent your relationship with us nor present any other false information about us;
  - **9.1.5** you do not otherwise use any "CloudSigma" trademarks and/or logos displayed on the Website without express written permission from us;
  - **9.1.6** you do not link from a website that is not owned by you; and
  - **9.1.7** your website does not contain content that is distasteful, offensive or controversial, infringes any intellectual property rights or other rights of any other person or otherwise does not comply with all applicable laws and regulations.
- **9.2** We expressly reserve the right to revoke the above permission to link to our Website where you are in breach of the Terms of Service and take any other action we deem appropriate. You shall indemnify us fully for any loss or damage suffered by us or any of

our associate companies where you are in breach of the above permission to link to the Website.

10.Termination

- **10.1** The Agreement shall commence on the Agreement Date and shall continue until terminated by you or us.
- **10.2** You or us may terminate the Agreement by giving thirty (30) days written notice (including without limitation email notice).
- **10.3** We may terminate the Agreement without notice to you and without providing any refund against your Credit Balance if any of the following occurs:
    - **10.3.1** the information you provided about yourself was false, materially inaccurate or incomplete;
    - **10.3.2** you were not 18 years old or did not have the legal capacity to enter into the Agreement at the time of submitting the Purchase for Services either in the capacity as an individual or on behalf of another person or legal entity;
    - **10.3.3** we are precluded from providing the Services to you by law or the decision of a competent legal or governmental authority;
    - **10.3.4** you do not use your account for a continuous period of three (3) months or more;
    - **10.3.5** your Credit Balance is zero (or negative) and you do not purchase any additional Credits within five (5) Working Days. In which case we shall additionally be entitled to immediately delete all data and information previously supplied as part of the Services and in relation to your account;
    - **10.3.6** a credit report indicates you no longer meet our reasonable criteria for creditworthiness;
    - **10.3.7** you are declared bankrupt, become insolvent, cease trading or otherwise are unable to meet debt and payment obligations as they fall due;
    - **10.3.8** you fail to pay any sum due to us as it falls due and do not remedy the overdue amounts within five (5) Working Days or receiving notice from us that you have amounts overdue;
    - **10.3.9** we reasonably decide that your ability to pay has been adversely affected including your credit or debit card being declined or us receiving notice of any disputed charges with your credit or debit card provider or your bank;
    - **10.3.10** you violate the Acceptable Use Policy;
    - **10.3.11** your death or the ceasing to exist of a legal entity where applicable; or
    - **10.3.12** you fail to comply with any provision of the Agreement and do not remedy the failure within twenty (20) Working Days of our notice to you outlining the failure.
- **10.4** If you do not have overdue funds on termination of the Agreement we will give you a reasonable opportunity to migrate your environment out of our Services in an orderly fashion where possible.
- **10.5** You may terminate the Agreement with us for breach of the Agreement by written notice if any of the following occurs:

- **10.5.1** we materially fail to provide the Services as agreed and do not remedy the failure within five (5) Working Days of receiving your written notice outlining the failure; or
- **10.5.2** we materially fail to meet any obligation under the Agreement and do not remedy the failure within twenty (20) Working Days of receiving your written notice outlining the failure.

- **10.6** Upon termination of the Agreement you:
  - **10.6.1** will not have access to any data stored on our network and infrastructure using the Services;
  - **10.6.2** must discontinue use of the Services;
  - **10.6.3** shall remain liable for any amounts outstanding including negative Credit Balance at the date of termination; and
  - **10.6.4** must relinquish use of any IP addresses and server names assigned to you by us in relation to the Services and also point any Domain Name Services away from us in relation to you.
- **10.7** Termination of this Agreement for whatever reason shall not affect:
  - **10.7.1** the accrued rights and liabilities of the parties arising in any way out of this Agreement at the date of termination including without limitation the right to recover damages against the other; and
  - **10.7.2** any provisions expressed to survive this Agreement, which shall remain in full force and effect.

11.Taxes, Duty and Value Added Taxation

- **11.1** All amounts payable for Services and Credits are stated exclusive of any VAT unless stated otherwise. We reserve the right and shall be entitled to charge VAT and other taxes and duty as appropriate.
- **11.2** You agree that you are liable for all taxes and duty resulting from your purchase of Credits from us and use of our Services.

12.Privacy Policy, Intellectual Property Rights and Confidential Information

- **12.1** All collection, storing and use of your data are governed by the Privacy Policy.
- **12.2** You agree acknowledge, accept and agree to be bound by the terms and conditions of the Copyright Notice.
- **12.3** Each of us retains all right, title and interest in and to our respective trade secrets, inventions, copyrights, and other intellectual property. Any intellectual property developed by CloudSigma during the performance of the Services shall belong to CloudSigma unless we have agreed with you in advance in writing that you shall have an interest in the intellectual property.

- **12.4** Additionally each of us agree not to use the other's Confidential Information except in connection with the delivery or use of Services, the exercise of respective legal rights with regards to the Agreement or as may be required by applicable law.
- **12.5** Each of us agrees not to disclose Confidential Information of the other to any third parties except:
    - **12.5.1** to our respective service providers, agents, and representatives, provided that such service providers, agents, or representatives agree to confidentiality measures that are at least as stringent as those stated in these Terms of Service;
    - **12.5.2** to law enforcement or government agencies when required to do so by law; and
    - **12.5.3** in response to a subpoena or other compulsory legal process provided that at least 5 Working Days notice period is provided prior to the disclosure unless prohibited from provided such notice in law.

13.Notices

- **13.1** All Services and the Website are operated and managed by CloudSigma. For routine communications regarding the Website or Services please contact us using the details provided on the Website.
- **13.2** Notices regarding termination of the Agreement or other legal matters should be sent by email and by recorded postal delivery to:
    - By Post:
      CLOUDSIGMA AG
      Sägereistrasse 35
      CH-8152 Glattbrugg
      Switzerland
      By Email: legal@cloudsigma.com
- **13.3** CloudSigma will give notice of amendments to the Acceptable Use Policy, Terms of Service, Privacy Policy, Copyright Notice and Service Level Agreement by posting them on the Website.
- **13.4** Notices for amendments to the Acceptable Use Policy, Terms of Service, Privacy Policy, Copyright Notice and Service Level Agreement are deemed received at the time that you next log in to the Web Console or the beginning of the first Working Day following the time delivered.

14.Disclaimer

- **14.1** We take all reasonable care to ensure that the information contained on the Website is accurate, however, we cannot guarantee its accuracy and we reserve the right to change the information on the Website (including these Terms of Service) at any time. You must therefore check these Terms of Service for any such changes each time you visit the Website or utilise the Services.

- **14.2** To the best of our knowledge, the information contained within the Website is accurate. Whilst we take reasonable care to ensure its accuracy, we make no representations or warranties of any kind with respect to the Website or the content contained on it, including any text, graphics, advertisements, links or other items. We will not be liable to any customer or member of the public for any information supplied on the Website. Our Website is, provided on an "as is" basis and we do not make any representations or warranties if such information subsequently proves to be inaccurate or out of date. Neither us nor any other contributor to the Website make any representation or gives any warranty, condition, undertaking or term either expressed or implied as to the condition, quality, performance, accuracy, fitness for purpose, completeness or freedom from viruses of the content contained on this website or that such content will be accurate, up to date, uninterrupted or error free.

15.Liability

- **15.1** All Services, software, content, images, materials and other data or information provided by us are done so 'AS IS'.
- **15.2** We make no representations or warranties whether express, implied, statutory or otherwise with respect to the services, software, content, images, materials and other data or information.
- **15.3** Except to the extent prohibited by applicable law, we disclaim all warranties including, without limitation, any implied warranties of merchantability, fitness for purpose, satisfactory quality, quiet enjoyment, non-infringement and any warranties arising out of the course of dealing or usage of trade.
- **15.4** We make no representations or warranties that the Services will be uninterrupted, error-free, or completely secure or that data stored using the Services will be secure or otherwise safe from loss or damage.
- **15.5** We shall not be responsible for any interruptions to the Services including but not limited to power outages, system failures or other interruptions including those that affect the acceptance and completion of payments for Purchases.
- **15.6** No advice or information obtained from us by you directly, via the Services or any third party shall create any warranty not expressly stated in these Terms of Service.
- **15.7** Nothing in these Terms of Service shall exclude or limit our liability for death or personal injury caused by negligence, fraud or any liability which cannot be excluded by applicable law.
- **15.8** We do not warrant and shall not be liable for any damage to, or viruses which may infect, your computer equipment or other property by reason of your access to, browsing or use of the Website.
- **15.9** We do not warrant that functions contained in the Services will be uninterrupted or error free or that defects will be corrected.

16. Limitation of Liability

- **16.1** Other than the payment obligations and/or indemnity obligations as set out in these Terms of Service liability of each party to the other arising from any given event or series of connected events shall be strictly limited to the amount paid by you to us during the immediately preceding month in which the event (or first in a series of connected events) occurred.
- **16.2** You acknowledge, accept and agree that the Service Level Agreement and Credits due under it from time to time are your sole compensation and recourse for damages and/or losses suffered by you and represent our total liability in relation to you in contract or tort (other than fraud) under the Agreement.
- **16.3** You acknowledge, accept and agree that neither party shall be liable in contract or tort (other than fraud) for:
    - **16.3.1** pre-contract or other representations;
    - **16.3.2** damages or losses as a result of disruption or interruptions of any kind to Services and any associated data loss or lack of availability; and
    - **16.3.3** loss of business, contracts, anticipated savings, loss of profit, loss of revenue, loss of goodwill, loss of reputation, loss or use of data or any indirect or consequential losses under any circumstances.

17.Indemnity

You shall indemnify and defend us, our agents, affiliates, suppliers, directors, officers, employees and partners (the "CloudSigma Indemnitees") from and against any legal claims, losses, liabilities, expenses, fines, damages and settlement amounts including reasonable legal fees and court costs incurred by CloudSigma Indemnitees arising under any claim as a result of your actual or alleged gross negligence, wilful misconduct, violation of law, failure to meet the security obligations required by the Agreement, violation of the Acceptable Use Policy or the Terms of Service. These indemnification obligations shall be enforceable provided that we promptly communicate to you reasonable details of any claim and cooperate in defending any claim. We will choose legal counsel to defend any claim provided these decisions are reasonable and communicated promptly to you. You must comply with reasonable requests from us for assistance and cooperation in defence of the claim. We may not agree to any settlement in relation to any claim without your prior written consent which may not be unreasonably withheld. Expenses incurred by CloudSigma Indemnitees must be paid by you as they are occurred.

18.Force Majeure

Neither of us will be in violation of the Agreement or liable for any loss or damage that the other may suffer because of any: act of God; power cut; power surge; fire, flood, earthquake, storm, hurricane or other natural disasters, war, invasion, act of foreign enemies, hostilities (whether war is declared or not), civil war, rebellion, revolution, insurrection, military or usurped power or confiscation, terrorist activities, nationalisation, government sanction, blockage, embargo, labour dispute, strike, lockout or interruption or failure of electricity or other utilities, or any other delay or failure caused by a third party. In such an event, we reserve the right to cancel or suspend the Website and/or our Services without incurring any liability.

19.Changes to the Agreement

- **19.1** We reserve the right to make changes to the Agreement including our Acceptable Use Policy, these Terms of Service, the Privacy Policy, the Copyright Notice and the Service Level Agreement, provided that changes are consistent with applicable law, industry norms and are reasonable. Any changes we make during the term of the Agreement will become effective to you in reference to all Services past, present and future when the earliest of the following occurs:
    - **19.1.1** you make a new/additional Purchase of credits that incorporates the revised Agreement;
    - **19.1.2** you exchange additional credits for our Services; or
    - **19.1.3** thirty (30) days after our notice to you describing the change.
- **19.2** If you do not wish to continue to use our Services following any such change you may terminate the Agreement by giving us written notice of termination on such grounds not later than thirty (30) days following the date that you were notified of the change. If you terminate the Agreement following such a change, thirty (30) days from the date of receipt by us of your written notice of termination:
    - **19.2.1** you may continue to use Services already exchanged for Credits until this point. Any Services not fully delivered at that time will be converted back to Credits and added to your Credit Balance based on the original rate of exchange used in relation to said Services; and
    - **19.2.2** you will be entitled to receive your current Credit Balance at that time as a cash refund from us on a one to one basis in the default currency of your account.

20.Further Terms

- **20.1** The illegality, invalidity or unenforceability of a provision of the Terms of Service under the law of any jurisdiction does not affect: the legality, validity or enforceability of any other provision of the Terms of Service in that jurisdiction; or the legality, validity or enforceability of that or any other provision of the Terms of Service under the law of any other jurisdiction.

- **20.2** If there is a conflict between the terms of any of the documents that comprise the Agreement, the documents will govern in the following order: Terms of Service, the Acceptable Use Policy, the Service Level Agreement, the Copyright Notice and the Privacy Policy.
- **20.3** The Agreement constitutes the entire agreement between you and us relating to the provision of the Service, and supersede any previous agreements, arrangements, undertakings or proposals, written or oral, between us in relation to this, and all past courses of dealing or industry custom. No oral explanation or information given by any party shall alter the interpretation of the Agreement. In agreeing to these Terms of Service, you have not relied on any representation other than those expressly stated in these Terms of Service.
- **20.4** You may not assign the Agreement without our prior written permission. We may assign the Agreement in whole or in part as part of a sale or corporate reorganization of our company and we may transfer your Confidential Information as part of any such transaction.
- **20.5** Any Purchase may be amended by a formal written agreement signed by both parties, or by an exchange of correspondence, including electronic mail, that includes the express consent of an authorized individual for each of us.
- **20.6** The relationship between you and us is one of independent contractors and the Agreement is not intended to create any type of partnership, joint venture, employee/employer relationship or franchise. Neither of us is an agent for the other and neither of us has the right to bind the other on any agreement with a third party.
- **20.7** The captions, section headings and titles in the Agreement are for convenience only and are not part of the Agreement.
- **20.8** We may use third party service providers to perform all or any part of the Services however we remain responsible to you under the Agreement for services performed by third party service providers to an equal extent as if we performed the third party services ourselves.
- **20.9** No delay and/or failure by us to enforce our rights or entitlements under the Agreement shall be deemed to be a waiver.
- **20.10** Other than as stated in these Terms of Service, the Agreement may be modified only by a formal document signed by both you and us.
- **20.11** Any waiver of any breach of the Agreement can only be made by us to you expressly in writing. No such waiver shall be considered a waiver of any subsequent breaches similar or otherwise.
- **20.12** Each of us acknowledges, accepts and agrees that we will not bring a claim against the other under the Agreement more than three calendar months after the time that the claim accrued.

21.Governing Law and Jurisdiction

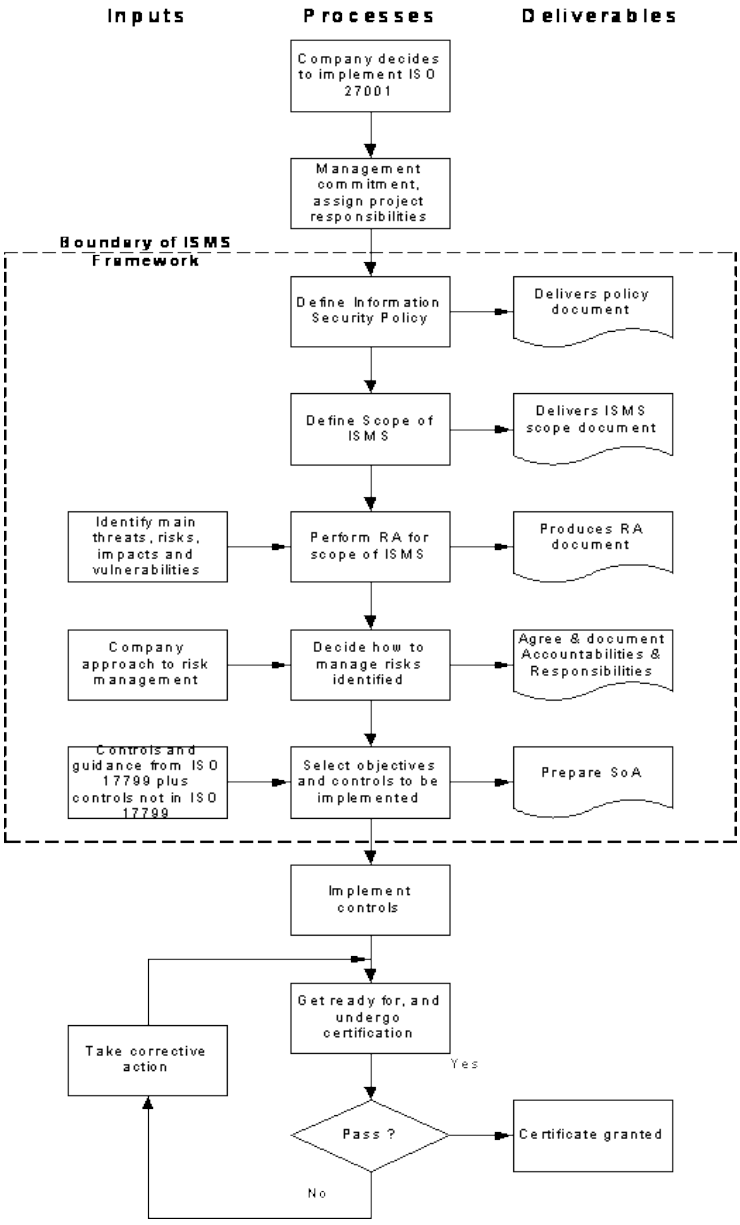
The Agreement and all other legal relationships between you and us will be governed by and construed in accordance with Swiss law. The courts of Zürich, Switzerland are to have exclusive jurisdiction to settle any dispute arising out of or in connection with the Agreement

and any proceedings will be brought in the courts of Zürich, Switzerland. We and you irrevocably submit and agree to submit to the jurisdiction of the courts of Zürich, Switzerland. The Agreement shall not be governed by the United Nations Convention on the International Sale of Goods. We and you irrevocably waive any objection which we or you may at any time have to the courts of Zürich, Switzerland being so nominated and agree not to claim that the courts of Zürich, Switzerland are not a convenient or appropriate forum.

Last Updated: 07 Oct 2011

Annex 8:

Table 1[246]



[246] http://www.27000.org/ismsprocess.htm" website accessed the 24th March 2012.