Cloud Computing Contracts

Regulatory Issues and Cloud Providers' Offer: An Analysis

Shyam S. Wagle

University of Luxembourg, 6, rue R. Coudenhove-Kalergi,
Luxembourg City, Luxembourg,
shyam.wagle.001@student.uni.lu

Abstract Cloud computing has recently emerged as a promising technology for IT industry. It is attracting small medium enterprises (SMEs) and big enterprises as it has "pay as per usage and SLA" provision in cloud computing. Contract terms in cloud computing help cloud users in decision making to enter into cloud environment. At the same time cloud users may face problems because of unclear terms and conditions or unbalanced terms and conditions, which are sometimes in the favor of cloud providers. Cloud contracts may not follow the existing regulations and contract law; in other words, it is not mandatory to fully adopt contract law in cloud computing contract. The paper presents regulatory challenges in cloud computing contracts and important issues to be included in cloud computing contract to make clear and transparent terms and conditions where both parties feel safe and fair. Another contribution of the paper is analyzing cloud contracts (Terms of service including Service Level Agreement (SLA)) offered by international cloud providers in respect with the standard guidelines recommended by different independent bodies to include in the cloud contracts. It also provides a visualized sorting table, which gives a clear picture of regulatory compliance status of the cloud providers in their cloud contract.

Keywords: Cloud Contract, Legal Issues, Compliance Status, SLA, Provider Analysis

1 Introduction

Cloud computing has recently emerged as a promising technology for IT industry. Small medium enterprises (SMEs) as well as big enterprises are attracted towards the cloud technology. Increasing number of IT service providers are offering computational, storage, networking, application hosting services to cover in several continents. There are many technical and legal challenges for all cloud users to fully adapt cloud computing in their business. Nevertheless, adopting cloud computing in their business has own pros and cons. Some institutions are attracted to cloud computing as easy deployment, low initial start-up cost and easily scalable, while others are serious about cloud adopting risks.

A contract is a legally binding agreement between two or more parties. In cloud contract there might be the agreement between cloud service providers and cloud users or together with other mediators (cloud broker, sub-contractors). Service level agreement (SLA) is a formal, negotiated document that defines (or attempts to define) in quantitative and qualitative terms the service being offered to the cloud users. Cloud service providers (CSPs) offer SLA with performances and service availability promises for their services. In practice, there are two contracting models [6] under which cloud providers provide services to the cloud users: 1) The online agreement is a click wrap agreement where user agrees the terms and conditions of the cloud providers as an "I agree" box or similar at the moment of service initiation. Online agreement is not subject to negotiate by cloud users. This model is the most commonly followed model by cloud provider where cloud users do not have any bargaining power to negotiate the standard agreement offered by cloud providers. This analysis is limited to an online agreement model because all the information mentioned here are taken from CSPs' website; (2) The second contract is standard, negotiated, signature based agreement, which generally occurs when larger companies want to move their critical data or applications to the cloud (for instance public cloud). In such agreement cloud users are free to push their terms and conditions as well as requirements according to them in the contract document.

Cloud users should feel comfortable and safe with in the agreement rather than blindly accept the terms and conditions proposed by CSPs, however, most of the small cloud users are not allowed to negotiate the cloud contract according to their choice. Cloud users and providers are often reluctant to take advantage of cloud computing services because they think either terms and conditions are unclear or are unbalanced in the favor of cloud providers[1]. More often cloud providers try to avoid their responsibilities like in security and data protection on the users to be in safe side from any legal obstacles but these are the current big issues in cloud computing contract from the legal point of view. In our observation, most of the cloud providers provides contractual issues under Terms of service and SLA section in their website.

In the survey conducted by W. K. Hon et al. [1] pointed out major six terms included in standard cloud computing contracts in which cloud users are most interested to negotiate: 1) Limitation of liability in data integrity and disaster recovery, 2) Service Level Agreement (SLA), 3)Security and privacy, 4)Vendor lock-in and exit, 5)Provider's ability to change the service features and 6)Intellectual property rights(IPR). It shows that cloud users are not yet convinced with current practiced standard cloud contracts. However cloud contract documents have neither standardized format nor terminology [9], and do not abide by any precise definition, notwithstanding some recent attempts [2] towards standardization.[2]

[1] $http://ec.europa.eu/justice/contract/cloud-computing/index_en.htm$

[2] https://ec.europa.eu/digital-single-market/en/news/cloud-service-level-agreement-standardisation-guidelines

The paper identifies the legal challenges in cloud computing from cloud contractual point of view. It provides the overview of Terms of service and SLA agreement offered by multiple international cloud service providers. It also provides the most important issues to be included in the cloud contract to make it safe and fair for both cloud providers and cloud users. In the end, it gives the most critical issues to be included, which are not considered by cloud providers in their contract agreement. As in the cloud contract most of the terms are related with data issues, the analysis is heavily influenced by EU data protection regime.

2 Regulatory Issues from cloud computing contractual point of view

As data of various cloud users is stored in a shared infrastructure environment, it is the possibility of accessing confidential data by un-authorized users or media. This cause many technical issues to protect data from unwanted access as well as it creates the legal issues due to dynamic nature of service access in cloud computing.

2.1 Data Privacy

The recently enacted EU's General Data Protection Regulation (GDPR)[3] repealing EU's Data Protection Directive 95/46/EC[4] gives fundamental rights to the data users(data subject) with respect to their personal data while requiring "data controllers" to follow rules and restrictions with respect to their data processing operations [10]. The Regulation is designed to further addressing new technological developments. Cloud users are entitled to inform the identity of any data controller and the purposes for which personal data are being collected or processed. According to EU's GDPR, data controllers should follow these main privacy protection principles of data protection that define the individual rights of the users and the responsibilities of data controllers that process personal data: fair and lawful processing, collection and processing only for a proper purpose, should be adequate, relevant and not excessive, should be accurate and up to date, should be retained no longer than necessary, giving the data subject access to his or her data, keeping data secure and no transfer of personal data to a country that does not provide an adequate level of privacy and personal data protection. New penalties (including fines of up to the greater of €100 million, or 2-5% of annual worldwide turn over) in the new regulation make cloud providers serious in regulatory compliance.

In the U. S., there is no comprehensive federal legislation to protect consumer's personal data and privacy. There is also not generally applicable regulations to limit the export of personal data outside U. S. considering as a "sensitive data" but "sensitive data" is to be considered for the data collected by online services

[3] $http://ec.europa.eu/justice/data-protection/reform/index_en.htm$
[4] http://eur-lex.europa.eu/legal-content/

about children under the age of 13; data collected by financial institutions about their customers; data collected by credit reporting agencies about consumers; and data collected by health care providers about patients [10].

In Australia, privacy issue is regulated by Privacy Act1988 (Cth). It is also applicable even it is done outside Australia if it relates to personal information about an Australian citizen, resident or related to Australia. This Privacy Act outlines national privacy principles, including a requirement that where personal information is collected, the record must be protected by reasonable security measures[5] and that generally information collected for one purpose should not be used for another[6] but it is not as strict as EU's data protection regulation related to the data privacy.

2.2 Trans-boarder Data Flow

Cloud service providers provide services to the users located in one or several countries; also, the first provider may outsource a portion of the processing to another cloud provider or may in turn be renting its cloud infrastructure from a bigger cloud provider [11]. All of these providers may be located in different countries or under different jurisdictions. There are three commonly used cloud computing deployment models: Private, Public and Hybrid which is the combination of private and public cloud. An additional model is a community cloud, which is less commonly used. From judiciary point of view, there are two cloud models: 1) Domestic Clouds: If a cloud is physically located under the same jurisdiction, it is a domestic or mono-jurisdictional cloud. In EU, a cloud is "domestic" or "mono-jurisdictional" if the conditions laid down by Article 4 of the GDPR are satisfied: either the controller is located within the EU or, it uses equipment located in the EU for purposes other than those of transit; 2) Trans-border clouds: If a cloud is not physically located under the same jurisdiction, it is a Trans-border or trans-jurisdictional cloud. In other words, the cloud, which does not fulfill the provision of domestic cloud it, is trans-border cloud.

The EU GDPR prohibits the transfer of personal data to countries, which do not ensure an adequate level of protection within the meaning of Article 25(2). Unless the data subject has given the previous consent unambiguously to the proposed transfer or under the condition that other procedures are in place, as per Article 26, data transfer outside European Economic Area (EEA) is not acceptable. Model Contracts, Safe Harbor Principle, Binding Corporate Rule (BCR) are the provisions for the personal data transfer outside EU.

2.3 Processor and Sub-processor Agreement

According to EU GDPR, processor of personal data must comply certain requirements when engaging in processing of personal data. There is still issue in cloud

[5] S14, National Privacy Principle 4.
[6] S14, National Privacy Principle 10.

computing, cloud provider is data processor or data controller [3]. Many providers are silent on the point or try to take their responsibility only as data processor. Many providers try to ensure they are not regarded as controllers (with greater obligation and liabilities) [1]. In cloud computing, there are many other service providers who act as cloud providers. Big cloud providers outsource multiple channels to sell their services. These multiple channels are also called reseller or service provider or outsourcer or cloud broker which acts as mediator of cloud provider and cloud users. Cloud broker may act as both cloud provider and cloud user because it can provide service to the end users integrating from multiple cloud providers as well as get cloud services form multi-cloud environment as a cloud users.

2.4 Governing Laws and Jurisdiction

As discuss in previous sections, cloud providers may have data center and service providing channels in different locations around the world. Cloud providers should comply and respect all the legal issues according to their national law to provide the cloud services to the users.

2.5 Data Subject Rights

It is a responsibility of cloud provider, to respond to data subject, if sh/e requests access to his/her personal data [1]. Behaving as a data processor, sometimes cloud providers want to skip such obligation of data subject. In such case, cloud provider points out users have direct access to and control their data and cloud provider does not have any role because they chose provider to process. This issue most often arrives because of unclear definition of cloud provider whether it is processor or controller.

3 Important Issues to be considered in Cloud Computing Contracts

The objective of the cloud contract is defining safe and fair term and conditions in the agreement, which is clear and transparent to every parties involved in the agreement. This section provides the most essential points to be included in cloud contracts.

3.1 Liabilities

Providers try to exclude liability altogether or restrict liability as much as possible because they provide commoditized services [1]. From provider's point of view also it is will not be practical to expose unlimited liability for small deal. For examples, liabilities of data loss of IaaS providers, liability for intellectual property rights infringement of software of SaaS providers are some examples conflicting issues mostly in between user and provider [1].

3.2 Service Level Agreement(SLA)

It is a documented agreement between the cloud service provider and cloud user that identifies services and cloud service level objectives. It should include minimum level objectives what cloud providers can provide to the cloud users and what happens when cloud provider failed to provide agreed minimum level objectives. Cloud Select Industry Group - Subgroup on Service Level Agreement (C-SIG-SLA) has defined a set of SLA standardization guidelines for cloud service providers and professional cloud users, while ensuring the specific needs of the cloud market and industry are taken into account.[7] This document is specifically targeted for European cloud market. We highlight here the major points to be included in the SLA agreement.

Performance Service Level Performance service level includes availability of the services (uptime, percentage of successful requests, percentage of timely service provisioning requests), response time of the service, capacity parameters (number of simultaneous connections, number of simultaneous cloud service users, maximum resource capacity, service throughput) and support (support hours, support responsiveness, resolution time).

Security Service Level In security service level, main important points to be included are: service reliability, authentication and authorization, cryptography, security incident management and reporting, logging and monitoring, auditing and security verification, vulnerability management and security control governance. Service reliability, which is directly interconnected with level of redundancy that cloud provider can provide user authentication and identity assurance level should be mentioned for authentication and authorization. How a cloud service provider handles information security incidents is of great concern to cloud service users, since an information security incident relating to the cloud service is also an information security incident to the cloud users. Incident reporting is also important in security incident management. Logging is the recording of data related to the operation and use of a cloud service. Monitoring means determining the status of one or more parameters of a cloud service. Logging and monitoring are ordinarily the responsibility of the cloud service provider.

Data Management Service Level From security and regulatory point of view, it is necessary to classify data, for example, user's data, provider's data, cloud service derived data and so on. It is also necessary to mention about data backup, mirroring and restore, lifecycle of data and data portability with different formats and interfaces.

[7] https://ec.europa.eu/digital-single-market/en/news/cloud-service-level-agreement-standardisation-guidelines

Personal Data Protection Service Level In SLA agreement, it is most important part to define cloud provider acts as a data processor or data controller or joint controllers (notably by processing personal data for their own purposes, outside of an explicit mandate from the user). It is also necessary describe applicable data protection codes of conduct, standards, certifications. If personal data are processed, it is necessary to define purposes of processing, openness, transparency o/f subcontractors, special categories of data. Document should define who is accountable on personal data breach. Another important point in data management service level is detail list about geographical location(s) where user data may be stored and/or processed and preferred geographical location for the storage of the user data. Last but not least, SLA agreement must define the access request response time period within which the provider shall communicate the information necessary to allow the user to respond to access requests by the data subjects.

3.3 Provider Lock-In and Exit

Lock-in is one of the top concern of cloud users. Most of the users may not wish to be locked-in for long time with an initial contract. Users should be free to leave the service after short specific time. User should be allowed to leave the service when he feels service is not appropriate to him or same service is available in the market in the cheaper price from other cloud provider. This is somehow commercial issue but main concern is how user's data and metadata can be recovered once service is terminated for whatever reason. Data formats should be easily accessible, readable and importable into other applications of other cloud providers independently. Data retention and deletion are also important issues in cloud contract. Users should be assured about retention of their data and complete deletion of their data after contract termination [1].

3.4 Term and Conditions

As usual like in other contracts there should be minimum term, renewals and notice periods. A long initial term may one of the issues of provider lock-in. Many of the cloud provider set automatic renewal provision, which may mislead cloud users if there is not a fix, notice periods. These terms and conditions depend on type services and types of business scale. Suspension rights must be also clearly mentioned in agreed contract.

3.5 Changing Service Features

Cloud providers should not be entitled to change terms without consent, or at least should give users notice and allow them to terminate.[8] Any changes in service must not adversely affect the previous commitment. Users must be notified with sufficient time mentioning the key changes and impact of changes.

[8] https://www.cloudindustryforum.org/search/site/CIF3

3.6 Intellectual Property Rights(IPR)

Intellectual property rights issues arise frequently on cloud processed data and, or applications. This generally happens due to not addressing properly who owns data in the cloud contract document.

4 Analysis of Term of Services and SLA committed by Cloud Service Providers

As cloud providers are increasing, cloud users have opportunities to select specific cloud services from multiple cloud providers. So, cloud broker exists between cloud provider and cloud users to facilitate both for the service delivery. Practically standard contract is feasible for big companies but making standard contract is for each SME for every cloud services is time consuming and costly for cloud providers. Cloud users also do not take more attention to make standard contract for a small cloud service subscription. Many of cloud providers offer online agreement even it is not negotiable and user agrees the terms and conditions of the cloud providers as an "I agree" box or similar at the moment of service initiation. Technically, the SLA agreement between cloud provider and cloud user is the legal document on which basis cloud user can claim for service credit or other incase of service infringement by cloud providers. In this paper, an overview of SLA offered by some international cloud service providers. Our observation of SLA agreement offered by most of the cloud providers shows that it is still incomplete and need to be provided detail information to avoid the conflict between cloud users and cloud providers or any third party involved in the agreement.

4.1 Terms of services and SLA provided by International Cloud Providers

SLA commitment is the main source of information, to cloud users, to choose services according to their requirements. In our observation, most of the cloud providers offer contract terms as "Terms of service" and "SLA". Some providers include SLA commitments in the terms of service and some providers provide SLA as a separate document. In this section, we provide the overview of cloud contract agreement (terms of service and SLA) committed by some commercially available cloud providers.

Microsoft Azure: Microsoft Azure[9] offers the specific SLA commitments in multiple services. Its SLA commitments range from maximum 99.99% to 99.9%. It provides the sector/region wise SLA commitments for cloud users. It has detail information regarding the data transfer, however, information in data privacy and security issues in term and conditions document is not well detailed.[10]

[9] https://azure.microsoft.com/en-us/support/legal/sla/summary/
[10] https://azure.microsoft.com/en-us/support/legal/services-terms-nov-2014/

GMOCloud: GMO Cloud[11] offers at least 99.999% monthly uptime for all cloud services. SLA document offered by GMO is not service specific commitments. It provides the details of security and backup, IPR but it is silent in data privacy and in governing law. Terms of service put liability to the cloud users to protect their privacy.[12] It also provides the detail information of data center locations.

HP Cloud: HP cloud[13] SLA offers range from at least 99.95% to 100% in the specific cloud services. It has lack of information in data privacy and security in its term of services. Its detail information of SLA and term of service is not easily available, as it is not planning to expand their public cloud service further.

Amazon: Amazon provide the different cloud services, however, Amazon S3[14] and Amazon EC2[15] are the most popular cloud services of Amazon. It offers at least 99.9% uptime for both S3 and EC2 services. It provides the well organized contract agreement for specific services[16,17]. Offered contract agreement contains detail information about security and data privacy, governing law and IPR.

RackSpace: Rackspace cloud[18] service provider also provides the service specific SLA commitments. Monthly uptime from at least 99.9% to maximum 100% is offered in their SLA document. It guarantees the user data privacy according to applicable data protection or privacy law.[19] It also provides the detail information of global security policy.

Google Cloud: Google cloud[20] offers service specific SLA. It ranges alteast 99.9% to 100% monthly uptime based on services offered. It covers most of the important terms in "Terms of Service". Data processing, security terms, compliance with different regulatory frameworks, governing law and jurisdiction are covered in terms of service[21]. SLA monitoring issues are still not clear in the committed document. It is possible to choose data center according to users preferences in different locations.

City Cloud: City cloud[22] offers the SLA commitments at least 100% monthly uptime in all the services irrespective of specific cloud service offers. It does not provide the detail terms of services related to security and data privacy, governing law and jurisdiction. It provides the geo-locations of data centers and monitoring facility of the services.

Cloud Sigma: Similarly, Cloud Sigma[23] also offers at least 100% monthly uptime irrespective of the multiple service offers. Terms of service define the

[11] *https* : *//www.gmocloud.com/common/download/catalog*$_i$*qcloud.pdf*
[12] http://us.gmocloud.com/legal/
[13] http://www.hpcloud.com/sla/
[14] http://aws.amazon.com/s3/sla/
[15] http://aws.amazon.com/ec2/sla/
[16] http://portal.aws.amazon.com/gp/aws/developer/terms-and-conditions.html
[17] http://aws.amazon.com/agreement/
[18] https://www.rackspace.com/information/legal/cloud/sla
[19] https://www.rackspace.com/information/legal/cloud/tos
[20] https://cloud.google.com/
[21] https://cloud.google.com/terms/
[22] https://www.citynetworkhosting.com/sla/
[23] https://www.cloudsigma.com/features/

liability privacy policy, IPR and confidential information and governing law and jurisdiction.[24] It also provides the information regarding cloud locations. However, terms and conditions are not clear enough as recommended in standard cloud contract guidelines.

Elastic Host: Elastic Host[25] also provides the service specific SLA offer ranges from at least 99.95% to 100%. It has lack of specific details in privacy and security issues in the provided SLA agreement and put more liabilities to the users. Proposed agreement is specific in governing law and jurisdiction.

Century Link Cloud: Century Link Cloud[26] is very specific in offering SLA commitments. It commits 100% uptime for public/private networks and at least 99.9% for rest of the services. It provides the privacy policy[27], data retention issues, Governing law and jurisdiction, however, it is not specific in data liability and other issues which are necessary to be a safe and fair cloud contract. It provides the data center locations in its website.

Digital Ocean: However, Digital Ocean[28] does not provide specific SLA commitments according to the service offers, it provides at least 99.99 % monthly uptime in network, power and virtual server availability. The offered document provides the information related to the liabilities, governing law, data privacy but a detail regarding the physical security is missing.

GoGrid Cloud: Go Grid Cloud[29,30] provides the very specific SLA commitments in each cloud service offered by it. It also provides the regional wise specific performance matrix in its SLA document. It is more specific in privacy and security issues, IP and third party offerings and choice of law and jurisdiction however it does not take more liabilities in user's data.

UpCloud: UpCloud[31] does not provide the specific SLA agreement to the users but gives the 100% monthly uptime guarantee to all the services irrespective of specific cloud service offers. Terms of service in the contract document is not clear on security and privacy, governing law and jurisdiction and data locations[32].

IBM Cloud: IBM does not provide the specific service wise SLA metrics. Terms of service of IBM is well organized and provides the details of security descriptions, data protection, conditions of transboarder data flow and information regarding the governing law and jurisdiction[33]. It also provides the information about the data center locations.

[24] https://www.cloudsigma.com/legal-switzerland/
[25] https://www.elastichosts.com/terms-of-service/
[26] https://www.ctl.io/legal/sla/
[27] https://www.ctl.io/legal/privacy/
[28] https://www.digitalocean.com/legal/terms/
[29] https://www.datapipe.com/gogrid/legal/sla/
[30] https://www.datapipe.com/gogrid/legal/terms-of-service/
[31] https://www.upcloud.com/blog/how-seriously-does-your-cloud-hosting-provider-take-redundancy/
[32] https://www.upcloud.com/documentation/terms/
[33] https://www-03.ibm.com/software/sla/

Exoscale Cloud: Exoscale cloud provides 95.95% availability in all services[34]. Terms of service are well described and clear. Document is specific on data security (however, it takes less liabilities), data protection and privacy, governing law and jurisdiction, Data storage and IPR.

Baremetal Cloud: It provides 99.999% availability unspecific with the cloud services. The SLA and terms of services[35] provided is not sufficient in data privacy, provider's liabilities, however, it provides the information regarding the physical level security and data center locations.

Arubacloud: Aruba cloud provides at least 99.95% availability for all the cloud services except 100% in power and air conditioning.[36] It provides the detail information about processing of personal data with specific applicable law, jurisdictions and competent but it provides the less information regarding the security issues from technical point of view. It also provides the information related to data center locations and monitoring details.

Softlayer Cloud: It does not provide the SLA commitment specific with particular services. In SLA agreement document, it uses a sentence "SoftLayer will use reasonable efforts to provide a service level of 100% for the public/private network..." but it guarantees the service credit more than 2 hours[37]. It is not clearly mentioned how it is provided, however, it agrees to maintain reasonable and appropriate measures related to physical security to protect user content[38]. The document is specific with data protection and privacy, governing law and jurisdictions. It also provides the geographical locations of data centers.

Vaultnetwork Cloud: The Vault network cloud endeavors to have service(s) available for access by any party in the world 99.5% of the time[39]. Provided document does not provide the detail about security, data privacy and protection. It is specific in governing law and jurisdictions.

CloudCentral: It provides the 99.95% uptime commitment for infrastructure services.[40] The terms and conditions[41] is clear in liabilities, governing law and IPR but there is not sufficient information in data privacy and physical security.

5 Legal and/or Major Missing Points in the Current Cloud Contracts Offered by Cloud Providers

The details of cloud contracts mentioned by multiple cloud providers are provided in section 4.1. We list out here some missing points, which are not properly addressed by cloud providers in their agreement, and some are against the

[34] https://www.exoscale.ch/terms/
[35] https://www.baremetalcloud.com/legal-terms
[36] https://www.arubacloud.com/company/general-conditions.aspx
[37] http://static.softlayer.com/sites/default/files/sla.pdf
[38] http://static.softlayer.com/sites/default/files/assets/page/Terms-of-Service.pdf
[39] https://www.vaultnetworks.com/about/company-policies/terms-of-service/
[40] https://www.cloudcentral.com.au/sla/
[41] https://www.cloudcentral.com.au/terms-and-conditions/

regulatory framework as mentioned in section 3, as important issues to be included in cloud contracts.

1. Lack of Transparency As we already discussed, there is not a standardized format of cloud contract. Cloud provider prefers to include terms according to their feasibility in the committed terms of services and SLA. Unclear and sometimes unfair terms in the cloud contract misguide the rights of cloud users in contract breaching. Lack of clearly monitoring technique in SLA, hidden payment obligation, automatic renewal occurs due to unclear terms in the cloud contract.
2. Lack of Liabilities and Indemnity Most of the providers claim their entire liability according to the charge paid by user or maximum amount. This is limiting or excluding legal rights of the user could be considered under some law (for instance under EU law it is considered as unfair contract [8])
3. Consent for the collection and processing of personal data for secondary non-compatible purposes Information for its internal purposes, such as billing or management of its cloud, gathered by cloud will belong to the cloud provider [12] but these information should not be used for the unfair advantage. In our analysis most of the providers do not mention theses issues in the agreement term but some provider still use these information for other purpose without particular consent from data subject [1].
4. SLA agreement

   a. Lack of Service Monitoring
   User pays as per usage in cloud computing. So, service credit and other claim will be authorized according to SLA agreement. Many of the contract terms do not mention about that is responsible for the service monitoring. SLA monitoring is challenging issue in recent days because cloud user may not provide services to the user according to SLA commitments [14]. There might be conflict in result of performance measurement between two parties if it is not clearly mentioned in the agreement.

   b. Disaster Recovery In the most of the contract document, how cloud providers manage disaster recovery is not clear. Well-managed disaster recovery plan of provider is very significant criteria when user select appropriate cloud provider.

   c. Location of Data In our observation, many of the provider provides the data center location in their website, but they do not mention about it in their terms of service and SLA. Cloud users can choose appropriate location if this information is included in SLA agreement.

   d. Data portability, Data irretrievability Very few cloud providers provide the information related to data portability and irretrievability. This information in SLA agreement makes cloud users for easily accessing data. Cloud users can easily retrieve their data if they need to switch to another cloud provider due to any reason.

Table 1. Criteria and sub-criteria for evaluating cloud services

Criteria	Sub-criteria	Short Name
Liabilities	Liabilities	*Li*
Performance Service Level	Availability	*Av*
	Response Time	*Res*
	Capacity	*Cap*
Security Service Level	Service Reliability	*Rel*
	Authentication and Authorization	*Au*
	Security incident mgmt	*inc*
	Reporting	*Rep*
	Logging	*Log*
	Monitoring	*Mon*
Data Management Service Level	Data Classification	*Dcls*
	Data Backup, Mirroring and Restore	*BMR*
	Data Lifecycle and Portability	*DLP*
Personal Data Protection Service Level	Code of Conduct	*Ccon*
	Purpose of Specification	*Pspec*
	Openness, transparency and notice	*OTN*
	Accountability	*Acc*
	Geographical Location of user data	*DL*
Provider Lock-in and Exit	Lock-in	*In*
	Exit	*Ex*
Terms and conditions	Terms and conditions	*TC*
Changing Service Features	Changing Service Features	*CS*
Intellectual Property Rights (IPR)	IPR	*IPR*

5.1 Pictorial Analysis of Cloud Provider's Contracts in Ordinary Values

SLA assured service brokering framework is proposed in [15]. This framework recommend the cloud services to the user with verified cloud services in performance delivery according to the SLA committed by cloud providers. Wagle et al. [16] and [14] proposed an evaluation techniques to evaluate the performance of the cloud providers. These papers are mainly focused on performance analysis of cloud providers. In cloud computing, specifically in a public cloud scenario, regulatory compliance management is also critical issue as the cloud users outsource data processing and storage to cloud providers that can be under legislation/regulation [13]. E Casalicchio and M. Palmirani [7] introduced legal compliance checking capabilities in cloud brokering but regulatory compliance status of the cloud providers are still not covered in the research. Information of service performance status including regulatory compliance status facilitates cloud users in decision making to choose cloud providers according to their requirements. The main motivation of this paper is analyzing the regulatory compliance of the cloud providers. We implement the heat map technique [4], [5], [14] proposed for performance evaluation to evaluate the regulatory compliance status of the cloud providers.

In Heat Map technique, potential cloud providers are sorted into marginal performance quantile classes to rank the providers with multiple performance criteria in increasing order or decreasing order. Performance quantile class is associated in the color form *dark red* (worst) to *dark green* (best) for the performance heat map visualization (See the color legend for 7-tiles in Table 2). We have considered major parameters described in section 3. All the information is taken from their websites. The developed heat map table gives the visualized table in what extent cloud providers are accepting regulatory compliance in their contract document.

Table 2. Pictorial View of Cloud Contracts offered by International Cloud Service Providers

criteria	Acc	BMR	Mon	Log	Rep	OTN	inc	Au	Rel	DL	Li	IPR	Ex	In	Res	TC	Pspec	Ccon	DLP	Dels	Cap	Av	CS
weights	0.33	0.33	0.33	0.33	0.33	0.33	0.33	0.33	0.33	0.33	0.33	0.33	0.33	0.33	0.33	0.33	0.33	0.33	0.33	0.33	0.33	0.33	0.33
tau(*)	0.52	0.52	0.52	0.52	0.52	0.50	0.49	0.49	0.49	0.34	0.26	0.09	0.04	0.04	0.02	0.00	0.00	0.00	0.00	0.00	0.00	-0.06	-0.34
Amazon Cloud	3	3	3	3	3	3	3	3	3	3	3	3	2	2	1	3	3	3	NA	NA	NA	3	0
Google Cloud Storage	3	3	3	3	3	3	3	3	3	3	2	3	0	0	1	3	3	3	NA	NA	NA	3	2
Microsoft Azure	3	3	3	3	3	3	2	2	2	2	2	2	1	1	1	3	3	3	NA	NA	NA	3	1
Aruba Cloud	3	3	3	3	3	3	3	3	3	3	0	2	0	0	1	3	3	3	NA	NA	NA	3	0
IBM Cloud	2	2	2	2	2	2	3	3	3	3	2	2	0	0	1	3	3	3	NA	NA	NA	2	0
City Cloud	3	3	3	3	3	3	1	1	1	3	2	2	0	0	1	3	3	3	NA	NA	NA	3	2
Rackspace Cloud	0	0	0	0	0	0	3	3	3	0	3	3	1	1	1	3	3	3	NA	NA	NA	3	1
CenturyLinkCloud	1	1	1	1	1	1	1	1	1	3	3	1	0	0	1	3	3	3	NA	NA	NA	3	2
Gogrid Cloud	0	0	0	0	0	0	2	2	2	3	0	3	1	1	2	3	3	3	NA	NA	NA	3	3
ExoCloud	0	0	0	0	0	0	3	3	3	3	0	3	0	0	1	3	3	3	NA	NA	NA	3	3
BareMetal Cloud	0	0	0	0	0	0	3	3	3	0	1	2	0	0	1	3	3	3	NA	NA	NA	3	2
SoftLayer Cloud	0	0	0	0	0	0	2	2	2	3	1	1	1	1	1	3	3	3	NA	NA	NA	3	NA
UpCloud	0	0	0	0	0	0	1	1	1	3	2	2	1	1	1	3	3	3	NA	NA	NA	3	2
Elastic Host	0	0	0	0	0	0	2	2	2	0	1	3	0	0	1	3	3	3	NA	NA	NA	3	2
DigitalOcean Cloud	0	0	0	0	0	0	2	2	2	2	1	2	0	0	1	3	3	3	NA	NA	NA	3	2
Cloudcentral Cloud	0	0	0	0	0	0	1	1	1	0	1	3	1	1	1	3	3	3	NA	NA	NA	3	NA
Cloud Sigma	0	0	0	0	0	0	1	1	1	3	1	2	0	0	1	3	3	3	NA	NA	NA	3	2
HP Cloud	0	0	0	0	0	0	1	1	1	0	1	2	1	1	1	3	3	3	NA	NA	NA	3	2
VaultNetwork Cloud	0	0	0	0	0	0	1	1	1	0	2	1	0	0	1	3	3	3	NA	NA	NA	3	2
GMOCloud-US	0	0	0	0	0	0	0	0	0	0	0	3	1	1	1	3	3	3	NA	NA	NA	3	2

Color legend:

quantile	0.14%	0.29%	0.43%	0.57%	0.71%	0.86%	1.00%

(*) tau: Ordinal (Kendall) correlation between marginal criterion and global ranking relation.

We assign 0 to 3 ordinary levels according to detail specification provided in the SLA document and Terms of service. If there is not any information provided, we assign 'NA' in that particular parameter. 3 - "Available, complete and included all the points", 2 - "Available, sufficient and missing some points", 1- "Avaiable, insufficient and missing some points", 0- "Availale, insufficient but not clear points" 'NA' - "Not Available"

We assign corresponding ordinal level according to fair and transparent contract document they have proposed to the users (See Table 1). The proposed visualized table gives an idea to cloud users, cloud brokers and regulatory bodies, how cloud providers are aware with regulatory compliance in contractual terms in cloud computing. First row in the the Table 2 gives the criteria of the evaluations. Second row represents the weight of the criteria. However, different weights can

be assigned for the evaluation according to the evaluator requirements, we have assigned equal weight in each sub-criteria considering all criteria are equally important. *tau* value represents the dominancy level of sorting(for instance 0.52 is dominancy level in this case). However, non of the cloud providers provide the information to make safe and fair contract, cloud providers *Amazon*, *Google Cloud Storage* and *Microsoft Azure* give more information in their cloud contract agreement than other cloud providers in selected providers in these comparisons (See Table 2). The ordinary levels and heat map table presented in this section is only for explanatory purposes (See Table 2) and should not be considered in any case as conclusive because expressing legal issues in quantitative value is not straightforward.

6 Concluding Remarks

Cloud contract is the most important legal binding document, which ensures fair and safe to all parties before delivering or receiving services in cloud computing. Obviously, it is not possible to cover all the terms and conditions in the contract document but it should be clear enough and fair for all parties involved in the agreement. Current cloud contract (terms of service and SLA) offered by cloud providers is not sufficient as a fair and safe and transparent cloud contract. The literatures, recommendation of different independent bodies and analysis of terms of service and SLA agreement committed by cloud providers show that cloud users are still not convinced with the current cloud contracts. The heat map table presented in this table gives the position of cloud providers according to their regulatory compliance status in their contract agreement. Visualized table of this information committed by multiple cloud providers helps cloud users to choose cloud providers according to their requirements and also helps cloud broker to recommend cloud providers according to users requirements. The potential future work includes the implementation of proposed heat map technique in SLA assured service brokering framework [15] which covers both service performance status and regulatory compliance status in service recommendation by cloud broker.

Acknowledgments I would like to thank LAST-JD program for financially supporting to perform this research. I am also thankful to Prof. Pascal Bouvry, Prof. Raymond Bisdorff for their valuable suggestions to prepare this paper.

References

1. Negotiating cloud contracts: Looking at clouds from both sides now. *STANFORD TECHNOLOGY LAW REVIEW*, 2012.
2. Elvira Albert, Frank de Boer, Reiner Hähnle, Einar Broch Johnsen, and Cosimo Laneve. Engineering virtualized services. In *Proceedings of the Second Nordic Symposium on Cloud Computing & Internet Technologies*, NordiCloud '13, pages 59–63, New York, NY, USA, 2013. ACM.

3. Paolo Balboni. *ISSE 2010 Securing Electronic Business Processes: Highlights of the Information Security Solutions Europe 2010 Conference*, chapter Data Protection and Data Security Issues Related to Cloud Computing in the EU, pages 163–172. Vieweg+Teubner, Wiesbaden, 2011.
4. Raymond Bisdorff. On polarizing outranking relations with large performance differences. *Journal of Multi Criteria Decision Analysis*, 20(1-2).
5. Raymond Bisdorff. The euro 2004 best poster award: Choosing the best poster in a scientific conference. In *Evaluation and Decision Models with Multiple Criteria*, International Handbooks on Information Systems. 2015.
6. Rajkumar Buyya, James Broberg, and Andrzej M. Goscinski. *Cloud Computing Principles and Paradigms*. Wiley Publishing, 2011.
7. Emiliano Casalicchio and Monica Palmirani. A cloud service broker with legal-rule compliance checking and quality assurance capabilities. In *1st International Conference on Cloud Forward: From Distributed to Complete Computing, October 6-8, 2015, Pisa, Italy.*, pages 136–150, 2015.
8. European Commission. Unfair contract terms, year = 1993, url = http://ec.europa.eu/consumers/consumer-rights/rights-contracts/unfair-contract/index-en.htm, accessed = 2016-04.
9. Elena Giachino, Stijn Gouw, Cosimo Laneve, and Behrooz Nobakht. *Theory and Practice of Formal Methods: Essays Dedicated to Frank de Boer on the Occasion of His 60th Birthday*, chapter Statically and Dynamically Verifiable SLA Metrics, pages 211–225. Springer International Publishing, Cham, 2016.
10. Nancy J. King and V.T. Raja. Protecting the privacy and security of sensitive customer data in the cloud. *CLaw and Security Review*, 28(3):308–319, 2012.
11. Maria Grazia Porcedda. *European Data Protection: In Good Health?*, chapter Law Enforcement in the Clouds: Is the EU Data Protection Legal Framework up to the Task?, pages 203–232. Springer Netherlands, Dordrecht, 2012.
12. Chirs Reed. Information Ownership in the cloud, year = 2010, url = http://papers.ssrn.com/sol3/papers.cfm?abstract-id=1562461, accessed = 2016-04.
13. Dirk Thatmann, Mathias Slawik, Sebastian Zickau, and Axel Küpper. *Towards a Federated Cloud Ecosystem: Enabling Managed Cloud Service Consumption*, pages 223–233. Springer Berlin Heidelberg, Berlin, Heidelberg, 2012.
14. S. S. Wagle, M. Guzek, P. Bouvry, and R. Bisdorff. An evaluation model for selecting cloud services from commercially available cloud providers. In *2015 IEEE 7th International Conference on Cloud Computing Technology and Science (CloudCom)*, pages 107–114, Nov 2015.
15. Shyam S. Wagle. Sla assured brokering (sab) and csp certification in cloud computing. In *Utility and Cloud Computing (UCC), 2014 IEEE/ACM 7th International Conference on*, pages 1016–1017, Dec 2014.
16. Shyam S. Wagle, Mateusz Guzek, and Pascal Bouvry. Cloud service providers ranking based on service delivery and consumer experience. In *4th IEEE International Conference on(CloudNet)*, pages 202–205, Niagara Falls, Canada, October 2015.