# Cloud Computing Contracts

Shyam S. Wagle

# Cloud Computing Contracts

## Regulatory Issues and Cloud Service Providers' Offers: An Analysis

Shyam S. Wagle

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

**Abstract** In cloud computing, a cloud service-brokering framework mediates between cloud service users (CSUs) and cloud service providers (CSPs) to facilitate the availability of cloud services to the users according to their requirements from multi-cloud environment. The current cloud service brokering framework considers the service performance commitments of CSPs, but it is not aware of current legal/regulatory compliance status of CSPs when recommending services to the users. A cloud contract (terms of service, Service Level Agreement (SLA)) helps cloud users in their decision making to select an appropriate CSP according to their expectations. CSUs feedback and survey report show that users are still not satisfied with the current terms and conditions committed to by CSPs. They believe that the terms and conditions are unclear or unbalanced, which they sometimes are when in favour of CSPs. In this paper, we identify some major issues to be included in cloud contract to make it safe and fair to all parties involved in the agreement from the European Union (EU) data protection perspective. Another contribution of the paper is analyzing cloud contracts (their terms of service and SLAs) offered by international CSPs in respect of the standard guidelines recommended by different independent bodies to include in the cloud contracts. This information is visualized in a sorting table, called a Heat Map table, which gives a clear picture of the regulatory compliance status of CSPs in their cloud contract documents.

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

## 1 Introduction

Cloud computing is a promising technology for the information technology (IT) industry that has only recently emerged. An increasing number of IT service providers are offering computational, storage, networking, and application hosting services that cover several continents. Small medium enterprises (SMEs) as well as big enterprises are attracted towards the cloud technology. Adopting cloud computing in their businesses has its pros and cons. Some institutions are

attracted to cloud computing because of its easy deployment, low initial start-up cost and easily scalablility, while others are serious about the cloud adopting risks. IDC[1] has forecasted that worldwide public cloud services spending will be to double by 2019. There are many technical and legal challenges for cloud users to fully adapt cloud computing in their businesses. In such circumstances, the actual service performance status of CSPs including regulatory compliance status according to the current legal framework, can help cloud users in their decision making to choose cloud services according to their requirements. A mediator, which can facilitate among cloud users to provide cloud services according to the businesses' requirements and finds appropriate users according to the services offered by them, is called cloud service broker (CSB). Mainly, it can play following roles [10], [14]:

- Discovery of SLA and law/regulation compliant services
- Monitoring run-time SLA and law/regulation compliance
- Checking of SLA and law/regulation compliance during the service on-board and at run time
- Actuation to maintain compliance.

Cloudforeurope[2] has identified the need for evaluating the performance of competing CSPs to select cloud services according to their requirements under the CloudWatchHub[3] project. The main idea is to accelerate and increase the use of cloud computing across the public and private sectors in Europe and educate SMEs how to choose the right service provider to take account of personal data protection and service level concerns as opposed to price only.

The reference document for CSBs to recommend cloud services to the users is a cloud contract document. Buyya et. al. [4] have pointed out two contracting models: 1) The online agreement is a click wrap agreement where the user agrees to the terms and conditions of the CSPs in an "I agree" box or similar at the moment of service initiation. Online agreement is not subject to negotiation by cloud users. This model is the most commonly followed model by cloud providers, where by cloud users do not have any bargaining power to negotiate the standard agreement offered by CSPs. This analysis is limited to an online agreement model because all the information mentioned here are taken from CSPs' website; (2) A standard, negotiated, signature-based agreement, which generally occurs when larger companies want to move their critical data or applications to the cloud (for instance to the public cloud). In such an agreement, cloud users are free to push their terms and conditions, and requirements, in the contract document.

In summary, a CSB can play two roles in a cloud computing architecture: 1) Service matching according the requirements of the cloud users, and 2) a regulatory compliance check according to the current legal framework. Current cloud service brokering frameworks recommend cloud services to the users by considering the service performance status of the CSPs, and most of these

[1] https://www.idc.com/
[2] http://www.cloudforeurope.eu/partners
[3] http://www.cloudwatchhub.eu

frameworks are not aware of the current legal framework. In the literature, most of the research works on the cloud service brokering are: 1) service performance service discovery and matching [13], Quality of Service (QoS) management and optimization [6], interoperability in multi-cloud architecture [5] and so on. Kousiouris et al. [12] and Casalicchio & Palmirani [7] have introduced legal compliance checking capabilities in cloud brokering but does not consider the service performance compliance in recommending cloud services to the cloud users. Wagle et al. [19] and [17] have proposed evaluation techniques to evaluate the performance of the CSPs. But, these papers are mainly focused on service performance analysis of cloud providers.

The current cloud service-brokering framework is not techno-legal friendly, which can be capable to check both legal and service performance compliance in a single platform. Cloud users and providers are often reluctant to take advantage of cloud computing services because they think that either the terms and conditions are unclear or are unbalanced in the favour of CSPs[4]. More often CSPs try to avoid their responsibilities, as in security and data protection for the users, to be on the safe side in terms of any legal obstacles; however, these are the current big issues in cloud computing contracts from the legal point of view. In our observation, most of the CSPs provides contractual issues under the terms of service and SLA section on their website. Our main source of information in analyzing the regulatory compliance status is: terms of service, SLA agreement, and any frequently asked questions (FAQ) available on the website of the cloud service provider.

In a survey conducted by W. K. Hon et al. [20], the authors pointed out six major terms included in standard cloud computing contracts, which cloud users are highly interested to negotiate. These are the: 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). The survey shows that cloud users are not yet convinced with current practiced standard cloud contracts. In cloud computing, cloud contract documents are yet to be standardized and develop defined standard terminology [9]; however, some recent attempts [1] towards standardization of cloud SLA have been performed[5].

The rest of the paper is organized as follows: Section 2 presents the overview of the SLA assured cloud service brokering framework. Section 3 identifies data protection risks in cloud computing from a cloud contractual point of view. We briefly present terms of service and SLA commitments offered by international cloud service providers to check the regulatory compliance status of them according to the current legal framework in Section 4. Based on it, we point out some important points to be included in a current cloud contract to make it safe and fair for both CSPs and cloud users. An approach to checking the regulatory compliance status of CSPs has been proposed as a main contribution

[4] http://ec.europa.eu/justice/contract/cloud-computing/index-en.htm

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

of the paper in Section 4.1. Since, in the cloud contract, most of the terms are related with data privacy issues, the analysis is heavily influenced by the EU data protection regime. The paper concludes with the overall concept in Section 5.

## 2 SLA Assured Cloud Service Brokering Framework

Figure 1 shows our proposed SLA assured cloud service brokering framework. The National Institute of Standards and Technology (NIST)'s cloud reference architecture [14] has defined specific roles for multiple actors in reference architectures. In the proposed SLA assured cloud service brokering framework, the cloud service broker (CSB) collects the requirements of users with their priority list of cloud services. The CSB then matches the offers of CSPs to provide services to the users according to these priority lists. The service monitoring module monitors the service performance of CSPs including regulatory compliance status of the CSPs. Wagle et. al [19], [17] have addressed service verification, service performance evaluation, sorting and ranking based on service performance monitoring, service performance pattern analysis, and pattern prediction for recommending optimal

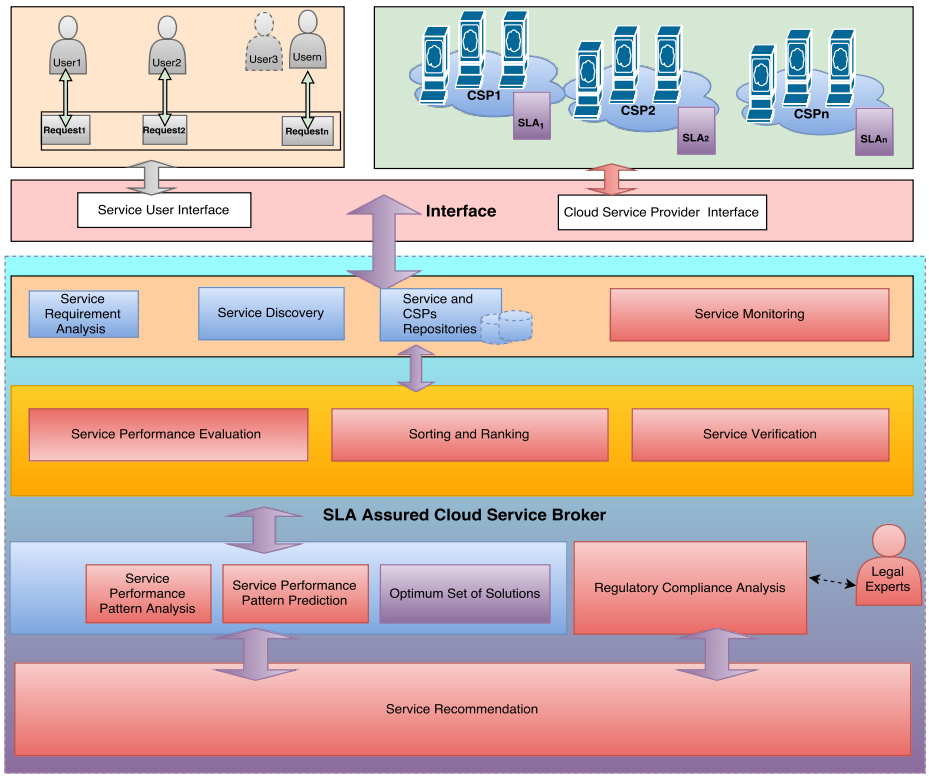


**Figure 1.** SLA Based Brokering and Service Verification Framework

sets of alternatives to the cloud users. In this paper, we mainly address the regulatory compliance status analysis of CSPs to recommend services to the users.

## 3 Safe and Fair Terms and Conditions in Cloud Computing

As the data from various cloud users is stored in a shared infrastructure environment, there exists the possibility of the accessing of confidential data by un-authorized users or media. This causes many technical issues to protect data from unwanted access as well as it creates legal issues due to the dynamic nature of service access in cloud computing. The recently enacted EU's General Data Protection Regulation (GDPR)[6] repealing the EU's Data Protection Directive 95/46/EC[7], gives fundamental rights to the data users (data subjects) with respect to their personal data while requiring "data controllers" to follow rules and restrictions with respect to their data processing operations [11]. The regulation is designed to further addressing new technological developments. Cloud users are entitled to be informed of the identity of any data controller and the purposes for which personal data are being collected or processed. According to the GDPR, data controllers should follow a main set of privacy protection principles on 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/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 either €100 million, or 2-5% of annual worldwide turn over) in the new regulation are intended to make CSPs serious about their regulatory compliance.

An Opinion of the Article 29 Working Party[8] has categorized data protection risks in cloud computing, into two major broad groups, 1) and 2): 1) risk due to a lack of control over the data. Under this category, lack of availability due to lack of interoperability (vendor lock-in), lack of integrity caused by the sharing of resources, lack of confidentiality in terms of law enforcement requests made directly to a CSP, lack of intervenability due to the complexities and dynamics of the outsourcing chain and data subjects' rights, and lack of isolation within the CSPs' clients are the main data protection risks, and 2) risk due to insufficient information regarding the processing operation (hence, a lack of transparency). Mainly these risks may arise from the controller not being aware of certain conditions: for example, that some form chain processing is taking place involving

[6] http://ec.europa.eu/justice/data-protection/reform/index-en.htm
[7] http://eur-lex.europa.eu/legal-content/
[8] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196-en.pdf

multiple processors and subcontractors, personal data are processed in difference geographic locations within the European Economic Area (EEA), and personal data are transferred to third countries outside the EEA.

However literature from many standardardization bodies and organizations have many points to be considered in the list to make the terms and conditions in the agreement safe and fair, following some major points addressed by the Cloud Select Industry Group - Subgroup on Service Level Agreement (C-SIG-SLA)[9]. In addition, the authors in [20] considered analyzing the regulatory compliance status of CSPs through the terms of service mentioned in the contract document, which is clear and transparent to every parties involved in the agreement. All the important points mentioned in the section that follows are represented in Table 1 as criteria and sub-criteria to analyze the regulatory compliance status of the CSPs.

### 3.1 Liabilities

Providers try to exclude liabilities altogether or restrict liabilities as much as possible because they provide commoditized services [20]. It is also true that it is not always practical to expose the CSPs to unlimited liabilities for a small deal. Liabilities of data loss of Infrastructure as a Service (IaaS) providers, liabilities for intellectual property rights infringement of software by Software as a Service (SaaS) providers are some examples of conflicting issues mostly between users and providers [20].

### 3.2 Service Level Agreement

A SLA is a documented agreement between the cloud service provider and cloud user that identifies services and cloud service level objectives (SLOs). It should include minimum level objectives that CSPs can provide to the cloud users and details about what happens when the CSP has failed to provide agreed minimum level objectives. The C-SIG-SLA has defined a set of SLA standardization guidelines for CSPs and professional cloud users, while ensuring the specific needs of the cloud market and industry are taken into account. This document is specifically targeted at the European cloud market. We highlight some major points, which are important to be included in a SLA agreement:

**Performance Service Level** The performance service level includes the 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).

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

**Security Service Level** Service reliability, authentication and authorization, cryptography, security incident management and reporting, logging and monitoring, auditing and security verification, vulnerability management and security control governance are the major points to be included in a security service level agreement. Service reliability, which is directly interconnected with the level of redundancy that a CSP can provide at the 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. 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 the security and regulatory point of view, it is necessary to classify data, for example, the user's data, provider's data, cloud service derived data and so on. It is also necessary to include data backup, mirroring and restore, lifecycle of data and data portability with different formats and interfaces in the agreement.

**Personal Data Protection Service Level** In a SLA agreement, the most important part is to define how the CSP 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 to describe applicable data protection codes of conduct, standards, and certifications. If personal data are processed, it is necessary to define the purposes of processing, openness and transparency of subcontractors. The document should define who is accountable for a personal data breach. Another important issue in the data management service level is a detailed list about the 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, a 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 concerns of cloud users. Most of the cloud users may not wish to be locked-in for long time with an initial contract. Users should be free to leave the service after a short, specific time. Users should be allowed to leave the service when they feel that the service is not appropriate for them or the same service is available in the market at a cheaper price from another CSP. While this is a commercial issue, the main concern is how a user's data and metadata can be recovered once the service is terminated for whatever the reason. Data formats should be easily accessible, readable and importable into other applications of

other CSPs, independently. Data retention and deletion are also important issues in a cloud contract. Users should be assured about retention of their data and the complete deletion of their data after contract termination [20].

### 3.4 Terms and Conditions

As usual, like in other contracts there should be minimum terms, a renewal period and a notice period. Long initial terms may be one of the issues of provider lock-in. Many of the CSPs set automatic renewal provisions, which may mislead cloud users if there are not a fixed notice periods. These terms and conditions depend on types of services and types of business scale. Suspension rights must be also clearly mentioned in an agreed contract document.

### 3.5 Changing Service Features

CSPs should not be entitled to change terms without consent, or at least should give users notice and allow them to terminate the contract[10]. Any changes in service must not adversely affect the previous commitment. Users must be notified within a sufficient time mentioning the key changes and impact of changes.

### 3.6 Intellectual Property Rights

Intellectual property rights (IPR) issues arise frequently in relation to cloud processed data and, or applications. This generally happens due to the issue of who owns data in the cloud contract document not being addressed properly.

## 4 Analysis of Terms of Service and SLA committed to by CSPs

In this section, we first provide the terms of service and SLA commitments of some incumbent CSPs. The main sources of information come from the terms of service, SLA document, security practices, privacy policies, the cloud documentations on getting started and other user guides, and FAQs by CSPs. We second expose some missing major items in the current cloud contracts. We third (in a following sub-section) offer two tables that explain these two sets of issues; the second table uses a simple pictorial format. What follows are the details in relation to the incumbent CSPs.

*Microsoft Azure:* Microsoft Azure[11] offers a specific SLA commitments in multiple services. Its SLA commitment ranges from maximum 99.9% to 99.99%. It provides sector/region-wise SLA commitments to the cloud users. It offers detailed information regarding the data transfer; however, information on data

[10] https://www.cloudindustryforum.org/search/site/CIF3
[11] https://azure.microsoft.com/en-us/support/legal/sla/summary/

privacy and security issues in the terms and conditions document is not clearly detailed[12].

*GMOCloud:* GMO Cloud[13] offers at least 99.999% monthly uptime for all cloud services. The SLA document offered by GMO is not a service-specific commitments. It provides details of security & backup, and IPR; however, it is silent on data privacy and governing law. The terms of service place the liability on the cloud users to protect their own privacy[14]. It provides detailed information of data centre locations.

*HP Cloud:* The SLA offer of HP Cloud[15] ranges from at least 99.95% to 100% in a specific cloud service. There is a limited information of data privacy and security in its terms of service. Detailed information of the SLA and terms of service are not easily available, as the company is not planning to expand its public cloud services further.

*Amazon:* Amazon provides various cloud services, however, Amazon S3[16] and Amazon EC2[17] are its most popular cloud services. It offers at least 99.9% uptime for both S3 and EC2 services. It provides a well organized contract agreement for specific services[18,19]. The contract agreement offered contains detailed information on security and data privacy, governing law and IPR.

*RackSpace:* Rackspace cloud[20] service provider provides a service specific SLA commitment. Monthly uptime from at least 99.9% to maximum 100% is offered in its SLA document. It guarantees the user data privacy according to applicable data protection/privacy law[21]. It also provides a detailed information on its global security policy.

*Google Cloud:* Google Cloud[22] offers a service specific SLA. It ranges from at least 99.9% to 100% monthly uptime based on the service offer. It covers most of the important terms in its terms of service. Data processing, security terms, compliance with different regulatory frameworks, governing law and jurisdiction are all covered in the agreement[23]. The SLA monitoring issues are still not clear, however, in the commitment document. According to the document, it is possible to choose data centre according to users' preferences in different locations.

*City Cloud:* City Cloud[24] offers a SLA commitment of at least 100% monthly uptime in all its services, irrespective of the specific cloud services. It does not provide detailed terms of service related to security and data privacy, governing

[12] https://azure.microsoft.com/en-us/support/legal/services-terms-nov-2014/
[13] *https* : *//www.gmocloud.com/common/download/catalog*$_i$*qcloud.pdf*
[14] http://us.gmocloud.com/legal/
[15] http://www.hpcloud.com/sla/
[16] http://aws.amazon.com/s3/sla/
[17] http://aws.amazon.com/ec2/sla/
[18] http://portal.aws.amazon.com/gp/aws/developer/terms-and-conditions.html
[19] http://aws.amazon.com/agreement/
[20] https://www.rackspace.com/information/legal/cloud/sla
[21] https://www.rackspace.com/information/legal/cloud/tos
[22] https://cloud.google.com/
[23] https://cloud.google.com/terms/
[24] https://www.citynetworkhosting.com/sla/

law and jurisdiction. It provides the geo-locations of data centres and monitoring facility of cloud services.

*Cloud Sigma:* Similarly, Cloud Sigma[25] also offers at least 100% monthly uptime irrespective of a specific service. The terms of service detail liability, privacy policy, IPR, governing law and jurisdiction[26]. Information related to data centre locations is also provided. However, the terms and conditions are not clear enough as is recommended by standard cloud contract guidelines.

*Elastic Host:* Elastic Host[27] provides a service specific SLA offer that ranges from at least 99.95% to 100%. It lacks specific details on privacy and security issues in the provided SLA agreement provided, and puts more liability on the users. The proposed agreement is specific in terms of governing law and jurisdiction.

*Century Link Cloud:* Century Link Cloud[28] is very specific in terms of its SLA document. It commits to 100% uptime for public/private networks and at least 99.9% for the rest of the services. It provides a privacy policy[29], data retention issues, governing law, and jurisdiction; however, it is not specific on data liability and other issues, which are necessary to make a safe and fair cloud contract. It provides data centre locations on its website.

*Digital Ocean:* However, Digital Ocean[30] 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 information related to the liabilities, and governing law, data privacy but a detail related to physical security is still missing in the document.

*GoGrid Cloud:* GoGrid Cloud[31,32] provides a very specific SLA commitment for each cloud service. It also provides a regional, specific performance matrix in its SLA document. It is more specific on privacy and security issues, IPR and third party offerings, and choice of law, and jurisdiction; however, it does not take more liabilities in user's data.

*UpCloud:* UpCloud[33] commit to a minimum of 100% monthly uptime to all services, irrespective of the specific cloud service. The terms of service are not clear on data security and privacy, governing law, jurisdiction, and data centre locations[34].

*IBM Cloud:* IBM does not provide specific service SLA metrics. The terms of service of IBM is well organized, and provides the details of security descriptions, data protection, conditions of trans-boarder data flow and information regarding

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

the governing law and jurisdiction[35]. It also provides information on data centre locations.

*Exoscale Cloud:* Exoscale Cloud provides 95.95% availability in all its services[36]. The terms of service are well described and clear. The 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 a cloud service. The SLA and terms of service[37] provided are not sufficient on data privacy or provider's liabilities; however, it provides an information related to physical level security and data centre locations.

*Arubacloud:* Aruba cloud provides at least 99.95% availability to all cloud services with the exception of 100% in power and air conditioning[38]. It provides detailed information on the processing of personal data with specific applicable law, jurisdictions and competency, but it provides the less information regarding the security issues from a technical point of view. It also provides an information related to data center locations and service monitoring details.

*Softlayer Cloud*: It does not provide a SLA commitment specific to particular services. In its SLA agreement document, it uses the sentence "SoftLayer will use reasonable efforts to provide a service level of 100% for the public/private network...", but it guarantees a service credit for more than two hours[39]. It is not clearly mentioned how this is provided; however, it agrees to maintain reasonable and appropriate measures related to physical security to protect user content[40]. The document is specific on data protection and privacy, governing law and jurisdictions. It also provides the geographical locations of data centres.

*Vaultnetwork Cloud*: The Vault network Cloud endeavours to have service(s) available for access by any party in the world 99.5% of the time[41]. The document provided does not detail security, data privacy and protection issues. It is specific on governing law and jurisdictions.

*CloudCentral:* It commits 99.95% uptime commitment to infrastructure services[42]. The terms and conditions[43] are clear in liabilities, governing law, and IPR, but there is not sufficient information on data privacy and physical security.

It is worthwhile to mention that cloud users still believe current contracts are not fair and remain favourable towards the CSPs. We identify here some major missing points in current cloud contracts, which can be helpful to improve the fairness and transparency of the cloud contracts. Four specific issues follow:

[35] https://www-03.ibm.com/software/sla/
[36] https://www.exoscale.ch/terms/
[37] https://www.baremetalcloud.com/legal-terms
[38] https://www.arubacloud.com/company/general-conditions.aspx
[39] http://static.softlayer.com/sites/default/files/sla.pdf
[40] http://static.softlayer.com/sites/default/files/assets/page/Terms-of-Service.pdf
[41] https://www.vaultnetworks.com/about/company-policies/terms-of-service/
[42] https://www.cloudcentral.com.au/sla/
[43] https://www.cloudcentral.com.au/terms-and-conditions/

1. Lack of Liabilities and Indemnity
   Most of the providers state their entire liability according to the charge paid by the user or a maximum amount. This could be considered to limit or exclude the legal rights of the user under some laws (for instance, under EU law it is considered to be an unfair contract [8])
2. Consent for the Collection and Processing of Personal Data for Secondary Non-Compatible Purposes
   Information that is collected from cloud users for the internal purposes of the CSPs, and gathered by them, such as billing or management of the cloud services, will belong to the CSPs [15]. However, this information should not be used for the unfair advantage. In our analysis, most of the providers do not mention theses issues in their terms of service, but some providers still use this information for other purpose without seeking the particular consent from the data subject [20].
3. Lack of Transparency
   As we already discussed, there is a lack of a standardized format and terminology of cloud contracts in cloud computing. Cloud providers prefer to include terms according to their feasibility in the proposed terms of service and SLA. Unclear, and sometimes unfair, terms of service in the cloud contract misguide the rights of cloud users in contract breaching. The lack of a clear monitoring technique in the SLA, hidden payment obligations, and automatic renewals can occur due to unclear terms of service in the cloud contract.
4. SLA agreement
   a. Lack of Service Monitoring
   The user pays as per usage in terms of cloud computing. So, service credit and other claims will be authorized according to the SLA agreement. Many of the contract terms do not mention about the methods of service monitoring. SLA monitoring has become a challenging issue, because it has been observed that all the cloud service providers may not provide services to the user according to their SLA commitments [17].
   b. Disaster Recovery
   In the most of the contract documents, how CSPs manage disaster recovery of the services is not clear. A well-managed disaster recovery plan is a very significant criterion for users who desire to select an appropriate CSP.
   c. Location of Data
   In our observation, many of the CSPs provide information related to data centre locations on their website. Cloud users can choose an appropriate location according to their requirements, but this information is not still part of the terms of service and SLA.
   d. Data portability, Data irretrievability
   Very few CSPs provide the information related to data portability and irretrievability. Cloud users should be easily able to retrieve their data if they prefer to switch to another CSP due for any reason.

Sometimes, it is hard for most of the cloud users to follow these points, since they are not aware of the existing legal framework or they do not have sufficient

legal knowledge to follow the legal framework. In the next section, we propose how a performance evaluation technique (called the Heat Map technique) can be implemented to check the regulatory compliance status of the CSPs. The Heat Map table (second of the two tables) gives complete information on the regulatory compliance status of the CSPs in a visualized form.

**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* |

### 4.1 Pictorial Analysis of CSP's Contracts in Ordinary Values

A SLA assured service brokering framework is proposed in [18]. This framework recommends the cloud services to the user that have a verified service performance delivery against the SLA commitments of CSPs. Wagle et al. [19] and [17] proposed evaluation techniques to evaluate the service performance of the CSPs. These two papers are mainly focused on service performance analysis of the CSPs. 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 CSPs that can be under legislation/regulation [16]. Casalicchio and Palmirani [7] have introduced a conceptual framework for legal compliance checking in cloud brokering, but the framework does not give a clear picture of

the regulatory compliance status of the CSPs. Information on service performance status, including regulatory compliance status, facilitates cloud users in their decision making to choose appropriate CSPs according to their requirements. The main motivation of our paper is analyzing the regulatory compliance status of the CSPs. We assign a corresponding ordinal level according to the fair and transparent contract document that the CSPs' have committed to the users (see Table 1. We then implement a Heat Map technique [2], [3], [17] proposed for service performance evaluation to evaluate the regulatory compliance status of the cloud providers. Using this Heat Map technique, potential CSPs are sorted into marginal performance quantile classes to rank the CSPs with multiple performance criteria in increasing order or decreasing order [17]. Performance quantile class is associated with the colours ranging from *dark red* (worst) to *dark green* (best) for the performance heat map visualization (See the colour legend for the 7-tiles in Table 2). We have considered the major parameters described in section 3 of this paper. All the information is taken from the CSPs' websites. The developed heat map table offers a graphic display, which shows to what extent CSPs are accepting regulatory compliance in their contractual documentation.

**Table 2.** Pictorial View of Cloud Contracts offered by International CSPs

| criteria | Acc | BMR | Mon | Log | Rep | OTN | inc | Au | Rel | DL | Li | IPR | Ex | In | Res | TC | Pspec | Ccon | DLP | Dcls | 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 the detailed specification provided in the SLA document, terms of service and so on. 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 - "Available, insufficient and missing some points", 0 - "Available, insufficient but not clear points" 'NA' - "Not Available".

We assign corresponding ordinal level according to fair and transparent contract document they have committed to the users (see Table 1). The proposed visualized table gives an idea to cloud users, cloud service brokers, and regulatory bodies of just how CSPs are aware of regulatory compliance in contractual terms in cloud computing. The first row in the Table 2 states the criteria of the evaluations. The second row represents the weight of the criteria. However, since different weights can be assigned to the evaluation according to the evaluator requirements, we have assigned an equal weight in each sub-criterion by considering that all criteria are equally important. The **tau** value represents the dominancy level of sorting (for instance 0.52 is the dominancy level in this case). However, none of the CSPs provide sufficiently complete information to make a safe and fair contract, although cloud providers *Amazon*, *Google Cloud Storage* and *Microsoft Azure* give more information in their contract document than other cloud providers in selected cloud providers in this regulatory compliance analysis (See Table 2). The ordinary levels and heat map tables presented in this section are only for explanatory purposes (see for example, Table 2) and should not be considered in any case as conclusive because expressing legal issues using quantitative value is not straightforward. It is worthwhile to mention here that this paper is only concerned with the transparency levels of the providers in terms of their contract document available on their website according to the current legal framework and does not check the service performance level of CSPs.

## 5 Concluding Remarks

A cloud contract is the most important legal binding document in cloud computing, which ensures fair and safe to all parties before delivering or receiving services. Obviously, it is not possible to cover all the terms and conditions in a cloud contract document, but any contract should nevertheless be clear enough to, and fair for all, the parties involved in the agreement. The cloud contracts currently committed to by CSPs do not seem to be sufficient as fair, safe and transparent cloud contracts. The available literature, the recommendations of different independent bodies, and an analysis of the terms of service and SLA agreements committed to by CSPs, show that cloud users are still not convinced about current cloud contracts. The heat map table presented in this paper gives the current position of CSPs according to their regulatory compliance status in their contract documents. A pictorial table of this information, committed to by the CSPs, helps cloud users in their decision making to choose an appropriate CSP according to their requirements. It also helps cloud service brokers to recommend CSPs according to users' needs. Potential future work includes an implementation of the proposed heat map technique in the SLA assured service brokering framework [18], which covers both service performance status and regulatory compliance status when recommending services to users.

**Acknowledgements** I would like to thank the LAST-JD programme for financially supporting to perform this research. I am also thankful to Prof. Dr. Pascal Bouvry and Prof. Dr. Raymond Bisdorff for their valuable suggestions in preparing this paper.

## References

1. 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, 2013.
2. Raymond Bisdorff. On Polarizing Outranking Relations with Large Performance Differences. *Journal of Multi Criteria Decision Analysis*, 20(1-2), 2013.
3. 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.
4. Rajkumar Buyya, James Broberg, and Andrzej M. Goscinski. *Cloud Computing Principles and Paradigms*. Wiley Publishing, 2011.
5. Rajkumar Buyya, Rajiv Ranjan, and Rodrigo N. Calheiros. Intercloud: Utility-oriented federation of cloud computing environments for scaling of application services. In *Algorithms and Architectures for Parallel Processing*, volume 6081 of *Lecture Notes in Computer Science*. 2010.
6. R. Calinescu, L. Grunske, M. Kwiatkowska, R. Mirandola, and G. Tamburrelli. Dynamic QoS Management and Optimization in Service-Based Systems. *IEEE Transactions on Software Engineering*, 37(3):387–409, 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, 1993.
9. Elena Giachino, Stijn de Gouw, Cosimo Laneve, and Behrooz Nobakht. Statically and Dynamically Verifiable SLA Metrics. In *Theory and Practice of Formal Methods - Essays Dedicated to Frank de Boer on the Occasion of His 60th Birthday*, pages 211–225, 2016.
10. Nikolay Grozev and Rajkumar Buyya. Inter-Cloud Architectures and Application Brokering: Taxonomy and Survey. *Soft. Pr. Exp.*, 44(3):369–390, March 2014.
11. 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.
12. George Kousiouris, George Vafiadis, and Marcelo Corrales. *A Cloud Provider Description Schema for Meeting Legal Requirements in Cloud Federation Scenarios*, pages 61–72. Springer Berlin Heidelberg, Berlin, Heidelberg, 2013.
13. Lei Li and Ian Horrocks. A Software Framework for Matchmaking Based on Semantic Web Technology. In *Proceedings of the 12th International Conference on World Wide Web*, WWW '03, 2003.
14. Fang Liu, Jin Tong, Jian Mao, Robert Bohn, John Messina, Mark Badger, and Dawn Leaf. NIST Cloud Computing Reference Architecture. 2011.
15. Chris Reed. Information Ownership in the cloud, 2010.
16. 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.

17. 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.
18. 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.
19. 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.
20. W.K.Hon, Christopher Millard, and Ian Walden. Negotiating Cloud Contract: Looking At Clouds From Both Sides Now. *Standford Technology Law Review*, 2012.