HAL
open science

The Role of SLAs in Building a Trusted Cloud for Europe

Ana Juan Ferrer, Enric Pages I Montanera

To cite this version:

Ana Juan Ferrer, Enric Pages I Montanera. The Role of SLAs in Building a Trusted Cloud for Europe. 9th IFIP International Conference on Trust Management (TM), May 2015, Hamburg, Germany. pp.262-275, 10.1007/978-3-319-18491-3_22 . hal-01416234

HAL Id: hal-01416234

https://inria.hal.science/hal-01416234v1

Submitted on 14 Dec 2016

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Distributed under a Creative Commons Attribution 4.0 International License

The role of SLAs in building a Trusted Cloud for Europe

Ana Juan Ferrer and Enric Pages i Montanera

Atos, Research and Innovation,
Diagonal. 200, 08018 Barcelona, Spain
{ana.juanf,enric.pages}@atos.net
http://www.atos.net

Abstract. The European commission recognises Cloud potential to improve competitiveness by enabling transformation to better connected and efficient society. However, still trust and security concerns hamper its massive adoption, both in private and public sectors. Towards a establishing a Trusted Cloud Europe this paper stresses the role that Service Level Agreements (SLAs) play by providing the mechanisms that allow both users and providers to establish a common understanding on the services to be provided and enforce guarantees around performance, transparency, conformance and data protection. To this end, the paper explores trust stakeholders and factors per cloud layer in the Cloud computing environment; it analyses the role of SLAs and provides a taxonomy of terms to support more tight and detailed SLA definitions that support users' requirements in order to improve reliability and transparency in Cloud.

Keywords: trust,cloud, sla

1 Introduction

Cloud Computing has reshaped the IT industry, and has the potential to change businesses and the economy by enabling higher IT efficiency and reliability. The European commission through the Steering Board of the European Cloud partnership [1] has recognised Cloud potential to boost growth, innovation and competitiveness in Europe [9] while enabling transformation to more connected and efficient society driving to benefits to citizens, business and public administrations alike.

For this to happen it is fundamental that Cloud services become reliable, trustworthy and secure for all users. The more extensive use of Cloud computing technologies bring to the users concerns on its data security, privacy issues and legal concerns, especially for public Cloud adoption. These concerns, in many cases are associated to intrinsic factors the nature of the Cloud computing model, such as multi-tenancy.

Service Level Agreements (SLAs) play a key role by being the mechanism that users have to enforce guarantees around performance, transparency, conformance

and data protection. As cloud adoption increases, cloud users, from both private enterprises and the public sector, will be seeking more tightly defined SLAs as a mean to build up dependable and trustworthy relationship terms with cloud providers.
This document first explores trust stakeholders and factors per cloud layer in the Cloud computing environment. Then, it analyses the role of SLAs. Finally it provides a taxonomy of terms to support more SLA detailed definitions [2], applicable to both private and public sector, aiming to support the development for trustworthy Cloud for Europe.

2 Cloud Computing Trust Stakeholders and Factors

Cloud computing differs from traditional IT security scenarios by its multi-tenant nature. Multi-tenancy refers to the ability for multiple customers (tenants) to share applications and/or infrastructure resources. This characteristic is the factor that allows Cloud providers to efficiently manage resource utilization among several users in a shared environment; and therefore, it is the enabler for providers to achieve economies of scale and commercial benefits.
However, it is the main source of concern for cloud users, if insufficient protection mechanisms are in place to guarantee security and privacy for both data and applications.
In the trustful provision and consumption of Cloud services, there is a difficult balance among confronted actors interests: cloud service providers and cloud users, where none of them can provide an overall solution for the issue at a general level. Depending on the nature of the cloud service offering (IaaS, PaaS, SaaS) providers are not aware of the contents and security requirements for the applications, while users, in the current state of development of Cloud, do not have sufficient vision of the security mechanisms and controls in place at providers facilities neither for detecting security incidents or holes. The following sections analyse specific security and trust factors in each Cloud layer by providing details on the specific issues and relevant research.

Software as a Service(SaaS)

SaaS completely decouples application execution from the users IT infrastructure. In this model, all application services are solely accessed by the user by a Web browser or thin client over the internet. While enterprise data is stored into the SaaS providers infrastructure, which can be based on a PaaS or IaaS provider or in a traditional infrastructure provisioning model. SaaS, despite being the Cloud model in which users information is more exposed to Cloud providers threats, given the complete loss of control from the user, is the lesser explored at security research levels, accounting for only a few references addressing concretely this topic [3, 4]. This can be motivated by the fact that SaaS applications are commonly delivered in the form of web applications for which security issues are a well-known and deeply analysed problem.

Platform as a Service (PaaS)

Nowadays, there is a truly diverse array of capabilities being offered as PaaS offerings. A PaaS cloud provides a container platform where users deploy and run their components. Diversities are present in supported programming tools (languages, frameworks, runtime environments and databases), in the various types of underlying infrastructure, and even on capabilities available for each PaaS. Taking the example of Google App Engine, Googles PaaS platform, it provides an execution environment where applications run on a virtualised technology foundation that scales automatically on demand. Google App Engine is often criticized for not providing transparency to the user to control infrastructure and how this infrastructure is used. Developers do not have direct control over resource allocation, because the underlying system and hardware resources are masked by the App Engine layer. Other existing PaaS platforms, such as Cloud Foundry automatize the application deployment to a set of template VMs, with complete and isolated platform stack. Vulnerabilities of these types of PaaS are the same than in IaaS environments.

Infrastructure as a Service (IaaS)

IaaS is by far the most analysed Cloud layer with regards security and data protection. In order to produce a systematic view on the question four different issues will be analysed separately: Security of Cloud APIs, VM repositories security and network issues. It has to be noted that security concerns on virtualisation technologies, are intentionally not further elaborated but in the context of public cloud IaaS implications.

- Security of API and interfaces: Cloud APIs or Cloud control interfaces are the means that the Cloud providers offer to manage VM images in an IaaS environment. They provide the capacities to add VMs, to modify them, as well as to manage their life-cycle (start, stop and resume). [4] analyses the security of these interfaces in a public Cloud environment, Amazon EC2, and a private Cloud management system, Eucalyptus. In it, two different classes of attacks XML Signature wrapping attacks and XSS attacks on browser front ends are demonstrated. It is important to notice that vulnerabilities in this aspect expose important security breaches of providers, given that the attacker get access to all virtual infrastructure of the user, and therefore its data.
- Security of VM repositories: Public VM repositories are a useful mechanism that both private cloud and public cloud providers can offer in order to simplify to users the task of creating their own VM images from scratch. Regardless of the usefulness of the mechanism, research demonstrates it can be a source of security risks both for the publisher or the image, the consumer and even the provider in which an instance of this VM is executed [5] in their work identify that the publisher can release sensitive information inadvertently. From both the receiver and the provider result is that they

get VMs that contain malicious or illegal content. [6] have performed an exhaustive analysis over a period of 5 months for all virtual images publicly available in the Europe, Asia, US East, and US West Amazon datacenters. In total 8.448 Linux images and 1202 Windows images were available. Of those available 5.303 images were analysed. The result of this analysis presented images containing software with critical vulnerabilities and leftover credentials.
- Secure Networking of VMs: Once again, the main source of concern about networking in public clouds is multi-tenancy. VMs from different customers may reside in the same physical network through which data traffic generated by VMs is transported. In order to overcome this issue techniques as network virtualization, through VLAN or other logical network segmentation are applied, so it segregates and isolates traffic among different user groups or subnets. However, some authors claim that these techniques were designed for the context of an enterprise, and therefore not securely applicable in the context of a public cloud due to limitations in the scale e.g. firewall policies ability to support load, or susceptibility to large scale DDoS attacks[7].

3 Users needs and requirements

Common concerns with regards cloud adoption; compliance, security, privacy and integrity, rely on the inability for users to measure, monitor and control activities and operations in Clouds third party platform or infrastructure. This is commonly understood as providers lack of transparency.
Improving transparency of Cloud services increases uptake of cloud, and this is beneficial for everyone: users and providers. A few concrete examples will help explain how benefits can be made by a dialogue between the different points of view to establish SLA model terms:

Benefits for Cloud Users:

- Provide mechanisms and a framework through which organizations make informed decisions when selecting a provider, using criteria such as: service availability, performance, monitoring, data privacy conditions, or penalties in case of SLA non-fulfillment.
- Compare Cloud Service levels with on-premise service levels (features and prices are easier to compare).
- Make informed decisions about Hybrid Cloud in the mix between public and private clouds.
- Easier ability for public sector to agree on EU-wide service expectations.

Benefits for Cloud Providers:

- Allow providers to make clear statements of differentiation by offering different levels of service at different prices.

- Open new avenues for innovative business models such as cloud brokerage and cloud aggregation.
- Make clear statements of differing cloud services from best effort to minimum commitment

In addition, for providers, the benefits anticipated by the development of detailed SLAs are twofold: First, by more concretely describing their services they can extend their usage levels thereby incrementing their customer base and profitability (enabled by economies of scale); Second, it can drive to richer Cloud scenarios by facilitating the development of Bursting, Brokerage or any type of multi-cloud scenarios. In these scenarios Cloud providers do not offer Cloud services themselves, but they rely on a more complex cloud ecosystem, enabling Cloud providers to offer better and more advanced services at a reduced price.
At all levels of its Stack (IaaS, PaaS, SaaS), the requirement of establishing adequate SLAs is to assure that both applications and infrastructure meet the promised performance and reliability benchmarks. This requirement is needed by any type of adopter, being applicable both for public sector and in general by any business environment or particular user.

- Allow providers to make clear statements of differentiation by offering different levels of service at different prices.
- Open new avenues for innovative business models such as cloud brokerage and cloud aggregation.
- Make clear statements of differing cloud services from best effort to minimum commitment

4 Service Level Agreements (SLAs)

SLAs specify cloud service provider and cloud service user consensus in the services to be provided.
From a legal perspective, SLAs are a binding contract among users and providers. Analysis of current SLAs offered by public Cloud providers performed in the context of the Cloud Legal project from Queen Mary School of Law Legal Studies [10] show clear limitations. It demostrates that many Cloud providers include elements in their Terms and Conditions asserting wide-ranging disclaimers of liability or of any warranty that the service will operate as described. In addition this research also found out that SLAs will often be couched in such terms as to exclude the majority of causes of a Cloud service outage, and will provide remedies only in the form of credits against future service. An additional remark done in the context of the OPTIMIS European research project [8] refers to the lack of clarity on how the layers of contract take into consideration the data subjects interests and rights where personal data are processed due to the complexity of cloud architectures and functions.

SLA terms must be defined in a way that all parties have the same understanding of what is being provided therefore, it is clear that the need for a

consistent definitions will only become more important as time goes on.

The following sections elaborate on SLA terms' taxonomy that aims to provide definitions relevant for the EU public and private sectors, based on common outsourcing practices that are applicable also to Cloud services cases.
These are structured according to three main categories: Access, Dependability and Security:

Access

- Availability of service
- Problem Resolution / Incident Response
- Reporting and Quality of Service
- Data Portability

Dependability

- Auditability
- Certification and Compliance
- Limitations
- Penalties

Security

- Data privacy conditions
- Security Provisions including backup and disaster recovery

4.1 Access

Access parameters refer to service characteristics details.

Availability of service

It is commonly understood as the degree of uptime for the service.

The ITIL [11] model provides the following definitions:

- A system is available when the customer receives the service stated in the SLA. The measurement and reporting of availability has to be based on a common understanding between the service provider and the service consumer.
- The degree of availability of a component or service is often expressed as the percentage of time for which the service is available. These figures can be determined in terms of downtime over a fixed period.
- Common formulas to calculate availability include:
  - Availability % =Actual Availability/Agreed Availability * 100
  - Actual Availability = Size of measurement interval Downtime
  - Downtime =Time to repair or Service restoration time detection time

ENISA [12] makes important remarks to be taken into account:

- SLA should clearly define when a service is considered available
- An SLA may define a recovery time objective (RTO), which is measured against mean recovery time (MRT)
- SLA may define MTBF (mean time between failures), which can be useful in the case where long periods of uninterrupted operation are critical

Problem Resolution / Incident Response:

Using ITIL Terminology [11]:

- An incident is defined as an event which is not part of the standard operation of a service and which causes or may cause disruption to or a reduction in the quality of services and customer productivity.
- A problem is a condition often identified as a result of multiple incidents that exhibit common symptoms. Problems can also be identified from a single significant incident, indicative of a single error, for which the cause is unknown, but for which the impact is significant. The primary objectives of Problem Management are to prevent Incidents from happening and to minimize the Impact of Incidents that cannot be prevented.

According to ENISA [12], the service level of a providers detection and response to incidents is often defined by means of:

- Severity: It has to be based in a well-defined scheme.
- Time to respond (from notification/alerting): the time to implement a remedial response.

Reporting and Quality of Service monitoring

Reporting refers to make available information in order to provide an overview of service performance and its operational status.

ENISA [12] provides the following classification of parameters:

- Service availability: Based on services' definition of availability. Examples of means to monitor this parameter are the following: relying on users, relying on providers' logs, by executing service health-checks, relying on providers' monitoring tools.
- Incident response: Examples of incident data to be provided include: time of first reporting incident discovery time, incident resolution time, incident severity, and affected assets.
- Service elasticity and load tolerance: the main aspect to monitor is the ability of the service to securely provision required resources when they are needed. It is proposed to verify it by means of regular testing. Depending on the nature of the provided service it can include: Number of CPU cores, CPU Speed, Memory size, VM quantity, VM storage, VM storage throughput, Bandwidth, Application response capacity.

- Data life-cycle management: It includes aspects such as: back-up test frequency and results, restoration speed, success or failure of operational back-ups, data recovery points, percentage of response to requests for data export successfully completed, data loss prevention system logs and system test results, data durability.
- Technical compliance and vulnerability management, such as: Information on patches and controls in place vs open vulnerabilities, information on compensating controls applied, data on specific vulnerabilities and trends, such as their classification and severity scores.
- Change management. Among others it may include: change notice time, change triggers, loss of certification status, changes or extension of jurisdictions in which data processing occurs, patches and major system changes, significant changes in security controls and processes used, time to implement security-critical customer change requests.

For the identified parameters, their reporting, based on the time-criticality of the information, can be provided based on three categories:

- Real-time service level data/feeds, including service level dashboards.
- Regular service level reports.
- Incident reports raised by the provider.

Data Portability

This refers to the users ability to create, copy and/or perform transmissions of data among cloud providers or between users facilities and a cloud provider.

Several initiatives and projects are working on developing and identifying common standards or frameworks for cloud solutions to increase the data and application interoperability between different cloud providers, such as the European Telecomunications Standards Institute (ETSI). Current lack of data interoperability standards, leads to significant effort for the customers to port data among providers in a usable format to avoid vendor lock-in.
usable format to avoid vendor lock-in. Article 18 of the draft Data Protection Regulation [13] specifically addresses this issue, by granting data subjects the right of data portability. So that, e.g. to transfer data from one electronic processing system to and into another, without being prevented from doing so by the controller. As a precondition and in order to further improve access of individuals to their personal data, it provides the right to obtain from the controller those data in a structured and commonly used electronic format. It is expected that this characteristic takes on a relevant role in cloud adoption in the future. The following parameters are proposed as part of the SLA:

- Data Format: Specification on structured and commonly used electronic formats available for the users to get its data from the provider.

- Data availability: Mechanisms in with data is made available, potentially including the specification of transport protocols and the specification of APIs, or any other mean, for the user to effectively get its data from the cloud provider.
- Data Sanitation Period: Transition at the end/termination of service: Period in which the data will be available in a usable format when the services are no longer needed or the service has terminated for any reason.
- Data Retention and Deletion clauses: Retention period for the provider to keep the data for the user, the period in which the provider is obligated to delete all personal data (including backups, Virtual Machine (VM) images, etc.) after service termination.

4.2 Dependability

Trust parameters reference parameters that allow determining the providers trust.

Auditability

Auditability refers to the ability of an organization, or defined systems or processes of the organization, to be evaluated on how the cloud computing service provider addresses the control frameworks of the specification.

A right to audit clause in a cloud SLA gives customers the ability to audit the cloud provider, which supports traceability and transparency. The goal of such an audit is to provide cloud service providers with a way to make their performance and security data voluntarily available. Using Audit specifications could provide a standard way to present and share information about performance and security needed by users to evaluate the service. Standardized information, in addition, could make comparison among providers easier.
Three different types of audit and assurance information can be provided by cloud providers to its users and reflected in SLA terms:

- Third-Party Attestations, Reports and Certifications: Reports and certifications produced by third-party auditors which attest to the design and operating effectiveness of the cloud provider environment such as: HIPAA, SOC 1/SSAE 16/ISAE 3402, SOC 2, SOC 3, PCI DSS, ISO 27001, CSA STAR.
- Documentation on procedures, standards, politics as well as configuration information, such as information about standard configurations and documentation for the current configuration of the users systems.
- Continuous logging and monitoring information. See Reporting and Quality of Service monitoring.

Certification and Compliance

Compliance refers to the act of fulfilling the requirements of a regulation.

Cloud providers privacy compliance is a major area of concern. Diverse initiatives are emerging in order to provide independent certification by reputable third parties so to provide a credible means for cloud providers to demonstrate their compliance with data protection principles. Besides, these initiatives could establish an assurance level to potential cloud users to evaluate providers level of privacy compliance. Among others, the following initiatives are highlighted:

- Safe Habor certification [14], as created under the EU-US Safe Harbor Programme refers to US companies aim to process personal data from the EU. It evaluates compliance with the Data Protection Directive. The certification is renewed annually, and failure to renew this certification implies that the provider directly loses Safe Harbor benefits.
- Cloud Security Alliance (CSA) Privacy Level Agreement [15] (PLAs), aim to define an extension to SLAs for privacy, in which the Cloud provider will clearly declare the level of privacy and data protection that it maintains with regards to relevant data processing. A Privacy Level Agreement (PLA) has a double aim: first, act as a tool for cloud users to assess a cloud providers commitment to address personal data protection and secondly, to offer contractual protection against possible damages due to lack of compliance by the provider with privacy and data protection regulation. The PLA Working Group recently published a PLA outline for the sale of cloud services in the EU that is based on the EU and the OECD privacy principles, and aims to provide a common structure for PLA worldwide.
- European Privacy Seal (EuroPriSe) [16], this certification is offered to manufacturers and vendors of IT products and IT-based services. The certification process is required of the evaluation of the product or service by legal and IT experts, as well as, the validation of the evaluation report by an independent certification body established at the Office of the Data Protection Commissioner of Schleswig-Holstein in Kiel, Germany.

The SLA could include terms to reflect compliance with data protection principles available, similarly to Third-Party Attestations, Reports and Certifications section with regards to Auditability.

Limitations

Limitations define the scope and restrictions of the provided service. Commonly it also defines providers liability terms.

These could include:

- Warranties and excluded warranties
- Disclaimer
- Liability

Penalties

SLA penalties define what will happen in the case that a provider fails to deliver the agreed service.

According to Web Services Agreement Specification (WS-Agreement), Penalties terms when present in a SLA express the penalty to be assessed for not meeting a business level objective. WS-Agreement specification [17] defines a language and a protocol for advertising the capabilities of service providers and creating agreements based on providers offers, and for monitoring agreement compliance at runtime. Violation of guarantee terms during an assessment window can incur certain penalties. The penalty assessment is measured in a specified unit and defined by a value expression, which can be assessed from service monitoring information. The WS-Agreement defines term language and SLA templates to express this parameter. Multiple research initiatives such as SLA@SOI, CLOUD4SOA, OPTIMIS, and others have assessed its applicability to Cloud environments [18].

4.3 Security

Security refers to parameters related to safety and protection mechanisms for cloud users.

Data privacy conditions

As reported by OPTIMIS European Research project [8], the Data Protection Directive makes clear that one of the main aims is the protection of fundamental rights and freedoms and in particular the right to privacy with respect to the processing of personal data. In addition, the Directive shall ensure the free flow of personal data between Member States.

The Directive deals with the processing of personal data. Personal data is defined as any information relating to an identified or identifiable natural person. As opposed to anonymous data, personal data is any information relating to persons who can be identified with reasonable effort. Although encrypted by technical means, this data is still considered personal. Anonymous data is data where the data subject can only be identified with an unreasonable amount of costs, capacities and time. This directive applies to the processing of personal data, going in detail through the terms:

- processing means any operation or set of operations which is performed upon personal data.
- addressee of the Data Protection Directive is the controller, this is the body which determines the purposes and means of the processing.

Whether data protection law is applicable depends on the establishment of the controller and the processor.

European Data Protection Directive is rather fragmented with regard to data security measures to be implemented by controllers and processors and the level of harmonization among different EU countries, where often technical and organizational data security measures are low. However, a minimum security requirements for cloud computing can be extracted. All measures mentioned aim to ensure confidentiality, integrity, authenticity and availability of the data. Destruction: Personal data must be protected against accidental or unlawful destruction to ensure integrity and availability as well as business continuity.

- Loss: The Data Protection Directive aims to protect the logical and physical availability of personal data by requiring the Member States to implement security measures against unplanned events (natural disasters, hardware failures).
- Alteration: Protection of personal data against alteration aims to ensure the authenticity and integrity of the data processed.
- Disclosure: One of the cornerstones of data protection is confidentiality of personal data. Therefore, the Data Protection Directive requires controllers and processors to protect personal data against disclosure.
- Access: Access to personal data must be controlled by specific security measures in order to maintain the confidentiality of personal data. Finally, data must be protected against all other unlawful forms of processing. This vague legal term aims to promote the use of privacy enhancing technologies when planning an information system designed to process personal data.
- State of the art: Security measures have to consider the state of the art.
- Appropriate measures: Security measures must be appropriate with regard to the anticipated risks inherent in the data processing, as well as with regard to the nature of data and the costs of their implementation

Based on this it is proposed to include the following terms in the SLA, using the terms provided by OPTIMIS project [19]:

- Data Protection Level:
  - None: when data is not sensitive, and it can be transferred without restriction.
  - DPA: Data can only be moved to countries that have a sufficient level of protection. It specifies whether the data included in the service under consideration is sensitive or not.
- Data Encryption Level: Defines data encryption algorithm to be applied (AES, Twofish,).
- Data Breach Notification: In addition, based on the proposal for a new data protection regulation and the obligation to notify data breach, SLA parameters to consider this are also included.
- Eligible Country List / Non Eligible Country List: Specific allowed and not allowed countries to host the data.

Security Provisions including backup and disaster recovery

ENISA [12] refers to these set of parameters as Data lifecycle management. It considers the group of parameters that measure the efficiency and effectiveness of the providers data handling practices (data export, data loss prevention and services back-up). Based on this SLA terms proposed under this category are the following:

- Back-up test frequency and results availability.
- Restoration speed: the time taken to obtain data from back-up from the time of request.
- Frequency of operational back-ups.
- Data durability: some providers specify a durability parameter which relates to the amount of data which can be lost in a time period.

5 Conclusions

SLA terms and taxonomy presented in this document aim to improve reliability and transparency in Cloud usage for all kinds of organizations. However, as remarked in the European Cloud Strategy [20], the public sector has a strong role to play in shaping the cloud computing market. As the EU's largest buyer of IT services, it can set stringent requirements for features, performance, security, interoperability and data portability and compliance with technical requirements.

Early cloud computing deployments for governmental agencies have demonstrated tangible benefits for both the public administration and the citizens. A very significant example in Europe is UKs G-Cloud Cloud store. This Government eMarketplace enables departments and organisations across the UK public sector to easily access centrally negotiated deals. At the time of writing this paper, it is on its sixth iteration, G-Cloud 6, with numerous accredited suppliers offering a high variety of services [21] to public-sector buyers. Among them, the percentage of SMEs is remarkable. Ovum research reports that the majority if contracts so far have focused on consultancy with Agile and Cloud enablement [22], and it is increasingly becoming the procurement mechanism of choice.

Generic benefits gained from adoption of cloud computing in Government, such as economies of scale, reduced maintenance costs, and the ability to leverage elastic and reliable computing infrastructures, have the potential to provide improved services in terms of reliability, availability, cost-efficiency and security.

In order to make reality of this potential, SLAs are a key tool, as they can provide transparency, assurance and therefore trust in European companies. Well-defined SLAs can offer fair and transparent conditions for Cloud service trading in Europe.

6 References

References

1. European Commision, DG Communications Networks, Content and Technology: Establishing a Trusted Cloud Europe (2014)
2. Mell, P., Grance, T.: The NIST Definition of Cloud Computing Recommendations of the National Institute of Standards and Technology (2011)
3. Software Progress, SaaS Security and privacy Whitepaper, (2008). Retrieved from http://community.progress.com/cfs-file.ashx/__key/communityserver-wikis-components-files/00-00-00-00-20/SaaS_5F00_Security_5F00_WP.pdf
4. Somorovsky, J., Heiderich, M., Bochum, R., Gruschka, N., Iacono, L. Lo. (2011). All Your Clouds are Belong to us Security Analysis of Cloud Management Interfaces, 314.
5. Wei, J., Zhang, X., Ammons, G. (2009). Managing security of virtual machine images in a cloud environment. Cloud computing security, (Vm), 9196. Retrieved from http://dl.acm.org/citation.cfm?id=1655021
6. Balduzzi, M., Zaddach, J., Balzarotti, D., Loureiro, S. (2012). A security analysis of amazons elastic compute cloud service on Applied Computing. Retrieved from http://dl.acm.org/citation.cfm?id=2232005
7. Popa, L., Yu, M., Ko, S. (2010). CloudPolice: taking access control out of the network. Proceedings of the 9th (1), 16. Retrieved from http://dl.acm.org/citation.cfm?id=1868454
8. OPTIMIS project, Cloud legal guidelines final report. Retrieved from http://www.optimis-project.eu/content/cloud-legal-guidelines-final-report
9. European Commission, MEMO/13/898 15/10/2013, What does the Commission mean by secure Cloud computing services in Europe?. Retrieved from http://europa.eu/rapid/press-release_MEMO-13-898_en.htm
10. Bradshaw, S., Millard, C., and Walden, I., 2010. Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services, Queen Mary School of Law Legal Studies Research Paper No. 63/2010. Retrieved from http://ssrn.com/abstract=166237
11. ITIL Availability Management: Beyond the Framework (2003). Retrieved from http://www.cmg.org/measureit/issues/mit33/m_33_1.html
12. European Network and Information Security Agency (ENISA), "Procure Secure, A guide to monitoring of security service levels in cloud contracts", 2012. Retrieved from http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/procure-secure-a-guide-to-monitoring-of-security-service-levels-in-cloud-contracts
13. European Commission, A proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) COM (2012) 11 final.
14. Safe Habor Regulation. Retrieved from http://export.gov/safeharbor/eu/eg_main_018365.asp
15. CSA Privacy Level Agreement Working Group. Retrieved from https://cloudsecurityalliance.org/research/pla/
16. European Privacy Seal. Retrieved from https://www.european-privacy-seal.eu/

17. Web Services Agreement Specification (2007). Retrieved from http://www.ogf.org/documents/GFD.107.pdf
18. Cloud Computing Service Level Agreements - Exploitation of Research Results (2013). Retrieved from https://ec.europa.eu/digital-agenda/en/news/cloud-computing-service-level-agreements-exploitation-research-results
19. Barnitzke, Benno; Ziegler, Wolfgang; Vafiadis, George; Nair, Srijith; Kousiouris, George; Corrales, Marcelo; Wldrich, Oliver; Forg, Nikolaus; Varvarigou, Theodora; Legal Restraints and Security Requirements on Personal Data and Their Technical Implementation in Clouds Workshop for E-contracting for Clouds, eChallenges ,2011.
20. COM(2012) 529 final, Unleashing the Potential of Cloud Computing in Europe. Retrieved from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:EN:PDF
21. G-Cloud raises the ceiling again for government IT procurement. Retrieved from http://www.computerweekly.com/news/2240208076/G-Cloud-raises-the-ceiling-again-for-government-IT-procurement
22. Ovum Research, UK G-Cloud to champion public cloud,. Retrieved from http://www.ovum.com/uk-g-cloud-to-champion-public-cloud/