REALIZATION OF A RESEARCH AND DEVELOPMENT PROJECT (PRE-COMMERCIAL PROCUREMENT) ON "CLOUD FOR EUROPE"

TECHNICAL SPECIFICATION: LEGISLATION EXECUTING CLOUD SERVICES

ANNEX IV (D)
TO THE CONTRACT NOTICE

TENDER NUMBER <5843932>
CUP <C58I13000210006>

CLOUD FOR EUROPE

FP7-610650

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 610650.

EXECUTIVE SUMMARY

Note: This is an informative summary of the document. The actual specification relevant for the bids is in the remainder of the document.

Adherence to legislation is a primary concern for public sector organisations. Various legal barriers exists, some of which can be addressed by technology. Therefore we have defined Legislation Execution to address or overcome some of these legal barriers. This may pave the way to cloud adoption by the public sector on a broader scale.

Legislation execution affects not only the behaviour of the cloud computing environment, but also the cloud actors (subjects and objects) involved. Compared with legislation-awareness, it takes enforcing the legislation in the cloud computing environment one step further. It does not only constrain the business to function in accordance with legal rules, but it also judges based on a set of rules, takes decisions and reacts. It is a judge, advocate and executor, all at the same time. Legislation execution is about reacting to illegal actions in order to enforce legislation by using technology.

This lot and the associated challenges propose a Legislation Execution framework to facilitate the development of such solutions. In addition Legislation Execution solutions are proposed, to be used in an operational cloud environment.

This document characterises the general requirements for this lot and the functional requirements for a framework and operational solutions.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

- None -

1 LEGISLATION EXECUTION

According to Table 1 of *Annex IV(A): Cloud for Europe: Challenges and General Requirements* this lot covers the challenges as listed in Table 1 below. An overview of all defined challenges and a short informative description is given in Annex IV(A). A detailed description and specification of the lot is given in the remainder of this document.

Table 1 - Legislation Executing Cloud Services lot challenges

Phase	No.	Challenge Summary	Lot	Award Criteria
Operation	7	Overcome, or address legal barriers to cloud computing	3: LE	I2, C2, Q1, Q4, Q6, Q8
	8	Enable the cloud development community to create and maintain legislation execution	3: LE	Q1, Q4, Q6, Q8
	11	Seamless change of service provider	1,2,3 (all)	Q1, I2, I3

LE = Legislation Execution

1.1 INTRODUCTION

In this section first an overview of the problem is provided. Then the benefits achieved when the solution gets deployed are described.

The current legislation brings certain barriers to cloud usage leading to no go decisions for cloud adoption. Since eliminating legal barriers may take a considerable time (if possible at all), we expect that another way of handling legal barriers is called for. We therefore propose to investigate which legal barriers can be overcome, or can be addressed by cloud technology.

Challenge 7**:** Overcome, or address legal barriers to cloud computing.

Challenge 7 is achieved by enforcing legislation in an operational cloud environment using technology. So challenge 7 is not about solving barriers via other means than technology.

Currently, there are various ways to handle legal barriers to cloud usage, for instance:

- adjusting and harmonising legislation
- creating new legislation
- making arrangements in contracts
- using codes of conducts
- and others

Another way of dealing with legal barriers could be to create innovative, technological cloud services that address or overcome the legal barriers. We therefore introduce *Legislation Execution* as functionality that does what the legislation requires. We define it as follows:

Legislation Execution is functionality that accomplishes certain requirements imposed upon cloud actors by national or international legislation during operation.

To introduce Legislation Execution further, the following text and examples serve.

A business service is realised by one or more business functions or processes. The functionality of Legislation Execution is to be found below the business process layer.

Legislation execution affects not only the behaviour of the cloud computing environment, but also the cloud actors (subjects and objects) involved. Compared with legislation-awareness, it takes enforcing the legislation in the cloud computing environment one step further. It does not only constrain the business to function in accordance with legal rules, but it judges based on a set of rules, takes decisions and reacts. It is a judge, advocate and executor, all at the same time. Legislation execution is about reacting to illegal actions in order to enforce legislation using technology.

Making a cloud service fully capable of legislation execution is at a complete new level, because this has to be done vertically, from infrastructure and application up to the business layer and horizontally, process by process.

Another wording for "Legislation Execution" is "Legislation Enforcement".

We expect that Legislation Execution results in functionality, suited to lower or eliminate legal barriers by using cloud technology, where and whenever possible. Such functionality is required by the public sector, as well as by the private sector. So for the industry there is a broad market consisting of both the private and the public sector.

The legal barriers, listed in Cloud for Europe's Deliverable D2.1, see [2], are a source of inspiration to design Legislation Execution to address or overcome these barriers.

We expect the following benefits to be achieved when Legislation Execution is deployed:

- More adoption and use of cloud computing by the public and the private sector
- Better service of the public and the private sector
- More effective legislation
- More user trust in cloud computing
- Less reliance on manual review and audits for adherence to legislation, combined with more coverage due to automation of enforcement, and less resource intensive enforcement of legislation.
- More transparency
- Better data protection
- Simpler contracts with cloud providers, since there will be less legal barriers to use cloud computing.

1.2 BUSINESS CONTEXT

In this section we first explain why research and development is needed. Then we describe the targeted impact of the aimed solution.

Currently, there are legal barriers that imply a "no-go" for cloud usage by the public sector. For instance, when a national government attorney points out to a public organization that certain data must be located on government premises, putting the data somewhere else is prohibited, and already outsourced data must even be taken back by the public organization. Assuming that such strong barriers are eliminated or addressed, cloud usage by the public sector is likely to increase. Exemplary work in the direction of the aimed solution has been published by the research community, for instance on enforcement of legislation in the Web environment. Note: the work presented under this subsection primarily serves for illustration purposes. Bidders are not bound to its content.

By Feng and Minjarez a description of a Web service is given for a patent for data protection, US patent No. US 007207067B2, see [1]. They describe 'a system and a method for enabling Web services to enforce multiple countries' data protection laws and regulations during data collection, data processing storage and data transfer.'

In *Bootstrapping Privacy Compliance in Big Data Systems*, see [3], a system to automate privacy policy compliance checking is described, consisting of a privacy policy language and a data inventory.

In general, Legislation Execution does not currently exist to our knowledge as commercial services, products, or other offerings for the cloud. Therefore, research and development is needed, followed by implementations of prototypes and further development towards commercial offerings.

The impact of the solution will be that the legislation, relevant in a cloud environment, will become more effective thus paving the way to broader cloud adoption by the public sector. Using Legislation Execution, legal barriers are affected in the following way:

1. some legal barriers will be eliminated,
2. some legal barriers will be addressed, and
3. some legal barriers will persist as they cannot be solved in a technical manner.

Impacts 1 and 2 on legal barriers will result in the benefits described above in the Introduction.

1.3 LOT-SPECIFIC REQUIREMENTS

This section describes the requirements that apply to all solutions offered for this lot.

The referenced actors are based on the definition of NIST[4], refer to the *Glossary* for the specification.

1.3.1 ***S3LR1*** *– USABILITY, COMPATIBILITY, LIMITATIONS*

The user community for Legislation Execution consists of cloud service providers and consumers. The cloud service providers may be public or private since some large governmental computer centres will function as cloud providers to their own and to other public organizations.

The aimed solution can take three forms from which the bidders may choose:

1. Framework. Having a framework (including methodology, guidelines and specifications), which describes how to make a process run in a legislation executing environment, would make things much easier for development and would ensure interoperability at the national and European level in this regard.
2. Generic Legislation Execution. This functionality can be combined with various business services in a flexible manner.

3. Legislation Execution that is associated and integrated with other business services.

For each of these three forms, the challenge and functional requirements will be specified in section 1.5. In Table 2 requirements are described which pertain to this lot for all three forms.

Table 2 - General requirements for this lot

ID	**S3LR1**
Actors	Cloud Provider, Cloud Consumer, Cloud End User
Description	Usability: The solution should be usable for public, private and hybrid clouds. Compatibility: The solution should be able to be used with the legislation and languages of the EU Member States. Limitations: The bidder must describe the limitations of the solution and must clearly state and describe the scope and applicability of the system. Costs across the lifecycle (acquisition, implementation, operation, decommission): The bidder should give a motivated estimation of costs across the lifecycle.
Applicable award criteria	Q1, Q4
Constraints	Existing patents should be respected.

1.4 USE CASE SCENARIOS

Below we present two use case scenarios of Legislation Execution, scenarios 1 and 2. Beyond that, a plenitude of other examples is conceivable. In Deliverable D2.1 *Legal Implications on Cloud Computing,* see [2], the following barriers in a public sector environment are described:

> '*(1) a patchwork of national conflicting laws resulting from local implementations of European legislation, with the European Data protection legislation as an area of focus, (2) fragmented and diverging national legislation in the public sector, with often no*

clear or even conflicting national legislation on whether data in the relevant domains can be transferred to a(n) (international) cloud environment, (3) national legislation discouraging the transfer of data to a(n) (international) cloud environment, (4) inappropriate public procurement legislation, and (5) hesitance to transfer data to the cloud for reasons of national defence and state secrets and, more in general, the extra-territorial enforcement and the foreign intelligence gathering practices.'

Refer to Deliverable D2.1 [2] for more details on legal barriers to address or overcome. Bidders are invited to describe their own use case scenarios for Legislation Execution. Note: the use cases scenarios presented under this subsection primarily serve for illustration purposes. Bidders are not bound to the contents of these scenarios.

1.4.1 ***S3UC1*** - *NOTIFICATION OF PRIVACY VIOLATION*

Whenever personal data is accessed in an unauthorized way (this could be by hackers, unauthorized employees of cloud providers or public sector organizations, or governmental intelligence surveillance), a notification of this occurrence is immediately and automatically sent to the cloud actors involved by the Notification of Privacy Violation. Although the notification does not prevent unauthorized access, the service reports it immediately, so that appropriate action can be taken by the relevant cloud actors or by the relevant systems. The notification functionality may decide to close down access to the data until appropriate action has been taken. This may help to increase trust and transparency in cloud services. Furthermore, it may also assist cloud users in finding out which cloud service providers are able to provide high quality clouds.

To describe a use case scenario of Legislation Execution, we provide a specific use case in Table 3. It provides more details on the Notification of Privacy Violation. This functionality is related to Privacy Laws to protect sensitive personal data.

Table 3 - Notification of Privacy Violation use case scenario

ID	**S3UC1**
Actors	Cloud Provider, Cloud Consumer, Competent Agency, Data Consumer
Description	Need: there is a legal requirement to get a notification when data is accessed in an unauthorized way. Benefits: more transparency, more trust, more effective legislation, better

	data protection. General functionality: whenever unauthorized access to data occurs (by hackers, unauthorized staff or intelligence surveillance), a notification is automatically sent to the data owner, and cloud service provider as well as to the competent authority, where applicable by particular case requirements[1]. Use case scenario: consider storage in the cloud of sensitive personal data. The "not yet 18 years old" child is living in a country where unauthorised access to the child's data has to be reported to competent authorities. No one will be able to access the data directly because the service is legislation-aware and will refuse the access to unauthorised people. However, backdoors might be found. The unauthorized person, or organization in the case of intelligence surveillance, will read the data, but thanks to a special technical solution[2], the system will automatically check (online or offline) and verify if the data access has been performed in conformance with legal requirements. Upon the violation of a specific legal rule, the system will react appropriately. For instance, it will act by alerting the cloud actors and competent authorities in accordance with the Privacy Law. The Legislation Execution may even decide to lock down the access until further investigations show what is going on with the data. Cloud actors can determine their line of action accordingly.
Constraints	

[1] The requirements to report unauthorized data access might be regulated by: 1) the law and agency processes 2) the specific rules/requirements of local agency in the terms of automated case reporting 3) the type/content of data.

[2] One example without the aim to prescribe a particular approach: the solution can be based on vertical integration of systems and services in such way that the actor related information is propagated through several system (access) layers or actors. For instance, the special file-system facility can log the access at storage level, aggregate, check, compare and process the logs from several sources, like web and file server, authentication facility etc. Upon the violation of specific legal rules, the system will react appropriately.

For the Notification of Privacy Violation the state of the art is that no automatic notification occurs simultaneously to data owner and cloud service provider. Some cloud service providers may inform their customers of hacking, but other types of unauthorized access to data is not always reported immediately, or is not reported at all, and also not automatically in a transparent way.

1.4.2 *S3UC2 - PERSISTENT LOCATION*

Persistent Location refers to the location requirements of sensitive data and ensures that such data does not leave the jurisdiction of a country, assuming the legislation of a country requires the data to reside on the countries territory where it falls under the jurisdiction of that country. Location persistence of data may also apply to a more limited area, such as the premises of a hospital, or the premises of a governmental data centre. When a cloud actor tries to transfer data to a location outside the scope of Persistent Location, the cloud actor is not allowed to do so by the technical solution for Legislation Execution, and the data owner receives a warning for further handling of these situations.

Table 4 - Persistent Location use case scenario

ID	**S3UC2**
Actors	Cloud Provider, Cloud Consumer, Competent Agency, Data Consumer
Description	Need: there is a legal requirement to have certain sensitive data reside in a specific location to adhere to a certain jurisdiction or because of certain organizational requirements. Benefits: more transparency, more trust, more effective legislation, better data protection. General functionality: keep data in a predefined location Use case scenario: In some cases and service provider environments, data might be intentionally (or automatically as well) dynamically transferred around provider data-centres based across diverse jurisdictions. The data transfer can be initiated for different purposes, such as attaining high availability, performing geo-replication, securing disaster recovery, backup, or improving end user data delivery and experience by employing Content

	Delivery Network, CDN, functionality. Some of these cases imply data multiplication and storage at different locations without the user's knowledge or consent. For instance, the data distribution for the purposes of CDNs might store the sensitive data on edge servers in different countries. Besides (1) the breach of the legal requirement for persistent location, it is not known or sure (2) who, when and how has accessed the data copies located at CDN's edge servers, or (3) what happens when the server has been decommissioned without securely deleting the data. Thus, the legislation execution in this example would not consider legislation execution at the original location only[3], but it will additionally enable service provider's edge servers to recognize the storage of sensitive data and react immediately and appropriately[4] upon the breach of legal requirements regarding the location of data.
Constraints	

For Persistent Location the state of the art is that the public sector chooses private or community clouds to guarantee the location of sensitive data. However, certain economic benefits cannot be realized in this way.

1.5 FUNCTIONAL REQUIREMENTS

This section describes the functional requirements of Legislation Execution. It consists of three subsections each defining a specific path to the project's goals of dealing with the legal barriers. General requirements pertaining to all three forms were described in section 1.3.

These functional requirements are not exhaustive in order to leave space for innovative work by the bidders. While the following subsections define approaches based on different abstraction levels, generality and applicability, they do not prescribe the outline or the order of the proposal. The bidder's proposal may conform to one of the three approaches (for instance a framework supported by tooling), or it may consist of their combination (for

[3] By not allowing to replicate or copy data to data-centers based in other countries.
[4] For instance, by determining the data owner, applicable legislation, and by executing the actions to be taken in the case of a breach.

instance a framework plus a generic Legislation Executing solution, created using the framework).

The referenced actors are based on the definition of NIST[4], refer to the *Glossary* for the specification.

1.5.1 *FRAMEWORK FOR LEGISLATION EXECUTION*

This section addresses Challenge 8: Enable the cloud development community to create and maintain Legislation Execution.

The purpose of this framework is to guide and facilitate development of Legislation Execution in order to overcome or address legal barriers to cloud usage. It should also allow developers to maintain Legislation Execution. The aim is to make the creation and maintenance easier, faster and more professional.

A framework is a 'Broad overview, outline, or skeleton of interlinked items which supports a particular approach to a specific objective, and serves as a guide that can be modified as required by adding or deleting items'.[5]

'In general, a framework is a real or conceptual structure intended to serve as a support or guide for the building of something that expands the structure into something useful. In computer systems, a framework is often a layered structure indicating what kind of programs can or should be built and how they would interrelate. Some computer system frameworks also include actual programs, specify programming interfaces, or offer programming tools for using the frameworks. A framework may be for a set of functions within a system and how they interrelate; the layers of an operating system; the layers of an application subsystem; how communication should be standardized at some level of a network; and so forth. A framework is generally more comprehensive than a protocol and more prescriptive than a structure"[6],

Table 5 - Functional requirements Framework

ID	Actors	Impor-tance	Applicable Award	Description	Depen-dencies

[5] Check http://www.businessdictionary.com/definition/framework.html for further details
[6] For more details: http://whatis.techtarget.com/definition/framework.

			Criteria And Questions		
S3FR1	Cloud deve-lopers	High	C2	The framework must at least consist of a methodology, guidelines and specifications.	
S3FR2	Cloud deve-lopers	Medium	C2, Q6	The framework can be supported by tooling, which can be tested in a pilot.	
S3FR3	Cloud deve-lopers	High	Q4	Input: The framework must be able to have as input laws and regulations of the EU and the Member States.	
S3FR4	Cloud deve-lopers	High	C2, Q6	Output: The framework must have as output guidance, possibly supported by tools for developers of Legislation Execution for cloud environments.	
S3FR5	Cloud deve-lopers	Medium	Q8	Performance indication: The bidder should indicate how the effectiveness of the framework can be measured, for instance faster development of Legislation Execution, higher quality of development etcetera.	
S3FR6	Cloud deve-lopers	Medium	Q1	Adaptation: The bidder should describe how the solution can be adapted, for instance to form a part of existing or emerging development frameworks.	

1.5.2 *GENERIC LEGISLATION EXECUTION*

This section addresses challenge 7**:** Overcome, or address legal barriers to cloud computing.

Here challenge 7 is addressed by enforcing legislation in an operational cloud environment using generic services that can easily be combined with various business services, which are used by the public sector. Bidders should feel free to come up with other Legislation

Execution functionality which carries out legislation in a cloud environment in combination with business services.

Table 6 - Functional requirements Generic legislation execution

ID	Actors	Importance	Applicable Award Criteria and Questions	Description	Dependencies
System, environment and the legal scope					
S3FR7	Cloud provider	High	Q1	The system must be provided as a separate solution, not tied to a specific business service or provider.	
S3FR8	Cloud provider, cloud consumer	High	Q1	The system must be usable with various business services with relevance to the public sector.	
S3FR9	Cloud provider, cloud consumer	Low	Q1	The system can be used under subscription, for instance in the form of cloud services which can be subscribed to in order to enforce legislation in a certain operational cloud environment.	
S3FR10	Cloud provider	High	Q4	The system must perform its functionality based on the set or subset of the laws and regulations of the EU and EU Member States.	
S3FR11	Cloud provider	High	Q4	The system must be able to recognize and conform to the various geographical levels of jurisdictions and their applicability under the context of a particular execution.	
S3FR12	Cloud provider	Medium	I2, Q4	The system should be able to comply with diverse levels of legislations, such as EU legislation, Member State legislation. It is able to evaluate and apply the	

				rules based on relevant principles, such as subsidiarity and precedence. It respects their scopes, interrelations and executes legislation based on that context.	
Legal rules conformance and maintenance					
S3FR13	Cloud auditor, cloud provider	High	Q4	While executing its rules, the system must provide the explanation in an appropriate form, making it possible to trace the rules, context, related factors leading to particular legal decision and execution.	
S3FR14	Cloud provider, cloud consumer cloud auditor	High	Q4	The authorized party must be able to maintain, alter and extend the legal execution component or its content in order to refine, expand or improve the legal rules applied in the context of the functionality. This process is transparent and traceable.	
S3FR15	Cloud provider, cloud consumer	High	Q4, Q8	The inspection and maintenance of legal rules and executions supported by the system must be possible for users of the system who are not deeply familiar with IT technologies.	
S3FR16	Cloud provider, cloud consumer	Medium	Q8	The maintenance of legal rules and executions supported by the system should be possible using user-friendly interfaces such as a web interface.	
S3FR17	Cloud provider, cloud consumer	Medium	Q6	The system should provide the API for maintenance of legal rules.	
S3FR18	Cloud provider, cloud	High	Q4	Stakeholders must be able to verify integrity, conformance and scope of the legal rules and regulations executed by the	

	consumer			service at any time.	
S3FR19	Cloud provider, cloud consumer	High	Q4	Stakeholders must be able to verify functionality and status of the legal execution service at any time.	
S3FR20	Cloud provider, cloud consumer	Medium	Q6	The service should hold all data related to successfully and unsuccessfully performed executions and provides the access to the relevant stakeholders.	
Core functionalities of the system					
S3FR21	Cloud provider, cloud consumer, cloud auditor	High	Q4	The system must perform conformance monitoring, auditing and the execution of legal processes, as defined by legal constraints and regulations. Upon the breach of those rules in the context of the particular data or services, the system must perform necessary legal and other activities.	
S3FR22	Relevant cloud actors	High	Q8	The system must inform the affected cloud actors upon the breach of legal rules related to its data or services.	
S3FR23	Cloud provider	High	Q1	The solution must be able to be adapted for use with current or emerging cloud services.	
S3FR24	Cloud provider	High	Q6	The solution must contain the complete documentation and description on how it can be integrated in current or emerging systems. The documentation contains architecture, design, use cases and examples, including the requirements posed on the service to be integrated with the solution.	
Analysis and cost related requirements					

S3FR25	Cloud provi-der	High	Q6	The solution must provide the metrics used to measure and present its functionality, such as effectiveness, efficiency, coverage, reaction times.	
S3FR26	Cloud provi-der	High	Q6	The solution must provide the metrics applied to measure its technical properties, such as performance, latency, impact and overhead.	
S3FR27	Cloud provi-der	Medium	Q6	The solution should provide a web interface, which enables the access to functional and technical metrics of its performances based on real-time or periodical reporting.	
S3FR28	Cloud provi-der	High	Q6	The solution must provide the analysis and estimates of incurred costs of the service, direct and indirect.	

1.5.3 *INTEGRATED LEGISLATION EXECUTION*

This section addresses challenge 7: Overcome, or address legal barriers to cloud computing.

Here challenge 7 is addressed by enforcing legislation in an operational cloud environment using services that are integrated with business services, which are used by the public sector, for instance an Enterprise Resource Planning system. This can be viewed as a first step towards Generic Legislation Execution, since this may be easier to develop.

Most of the functional requirements are similar to the Generic Legislation Execution, except for some requirements, S3FR8 and S3FR9, and S3FR29, which are different. For completeness sake the functional requirements are listed below with the requirement identification S3FR xx.

Table 7 - Functional requirements Integrated Legislation Execution

ID	Actors	Impor-tance	Applicable Award Criteria and Questions	Description	Depen-dencies

System, environment and the legal scope					
S3FR29	Cloud provider	High	Q6	The system must be provided as the solution integrated into the cloud provider's business service offering relevant for public administrations.	
S3FR30	Cloud provider	High	Q4	The system must perform its functionality based on the set or subset of the laws and regulations of the EU and EU Member States.	
S3FR31	Cloud provider	High	Q4	The system must be able to recognize and adhere to the various geographical levels of jurisdictions and their applicability under the context of a particular execution.	
S3FR32	Cloud provider	Medium	I2, Q4	The system should be able to comply with diverse levels of legislations, such as EU legislation, Member State legislation and jurisprudence. It is able to evaluate and apply the rules based on relevant principles, such as subsidiarity and precedence. It respects their scopes, interrelations and executes legislation based on that context.	
Legal rules conformance and maintenance					
S3FR33	Cloud auditor, cloud provider	High	Q4	While executing its rules, the system must provide the explanation in an appropriate form, making it possible to trace the rules, context, related factors leading to particular legal decision and execution.	
S3FR34	Cloud provider, cloud consumer, cloud auditor	High	Q4	The authorized party must be able to maintain, alter and extend the legal execution component or its content in order to refine, expand or improve the legal rules applied in the context of the functionality. This process is transparent and traceable.	

S3FR35	Cloud provi-der, cloud consu-mer	High	Q4, Q8	The inspection and maintenance of legal rules and executions supported by the system must be possible for users of the system who are not deeply familiar with IT technologies.	
S3FR36	Cloud provi-der, cloud consu-mer	Medium	Q8	The maintenance of legal rules and executions supported by the system should be possible using user-friendly interfaces such as a web interface.	
S3FR37	Cloud provi-der, cloud consu-mer	Medium	Q6	The system should provide the API for maintenance of legal rules.	
S3FR38	Cloud provi-der, cloud consu-mer	High	Q4	Stakeholders must be able to verify integrity, conformance and scope of the legal rules and regulations executed by the service at any time.	
S3FR39	Cloud provi-der, cloud consu-mer	High	Q4	Stakeholders must be able to verify functionality and status of the legal execution service at any time.	
S3FR40	Cloud provi-der, cloud consu-mer	Medium	Q6	The service should hold all data related to successfully and unsuccessfully performed executions and provides the access to the relevant stakeholders.	
Core functionalities of the system					
S3FR41	Cloud provi-der, cloud consu-mer, cloud	High	Q4	The system must perform conformance monitoring, auditing and the execution of legal processes, as defined by legal constraints and regulations. Upon the breach of those rules in the context of the particular data or	

	auditor			services, the system must perform necessary legal and other activities.	
S3FR42	Relevant cloud actors	High	Q8	The system must inform the affected cloud actors upon the breach of legal rules related to its data or services.	
S3FR43	Cloud provider	High	Q1	The solution must be able to be adapted for use with current or emerging cloud services.	
S3FR44	Cloud provider	High	Q6	The solution must contain the complete documentation and description on how it can be integrated in current or emerging systems. The documentation contains architecture, design, use cases and examples, including the requirements posed on the service to be integrated with the solution.	
Analysis and cost related requirements					
S3FR45	Cloud provider	High	Q6	The solution must provide the metrics used to measure and present its functionality, such as effectiveness, efficiency, coverage, reaction times.	
S3FR46	Cloud provider	High	Q6	The solution must provide the metrics applied to measure its technical properties, such as performance, latency, impact and overhead.	
S3FR47	Cloud provider	Medium	Q6	The solution should provide a web interface, which enables the access to functional and technical metrics of its performances based on real-time or periodical reporting.	
S3FR48	Cloud provider	High	Q6	The solution must provide the analysis and estimates of incurred costs of the service, direct and indirect.	

2 REFERENCES

[1] A. Feng and F. Minjarez, “Enforcing data protection legislation in Web data services,” U.S. Patent 007207067B2, April 17, 2007.

[2] L. Hellemans et al. Legal Implications on Cloud Computing. Brussels, Cloud for Europe Deliverable D2.1, 2014. Available: http://www.cloudforeurope.eu

[3] S. Sen et al. (2014) *Bootstrapping Privacy Compliance in Big Data Systems*. Available: http://www.saikat.guha.cc/pub/oakland14-bootstrappingprivacy.pdf

[4] NIST, NIST Cloud Computing Reference Architecture, Special Publication 500-292, 2011