Cloud Service Level Agreement Standardisation Guidelines

Brussels

24/06/2014

Table of Contents

Preamble

Cloud Service Level Agreements (Cloud SLAs) form an important component of the contractual relationship between a cloud service customer and a cloud service provider of a cloud service. Given the global nature of the cloud, SLAs usually span many jurisdictions, with often varying applicable legal requirements, in particular with respect to the protection of the personal data hosted in the cloud service. Furthermore different cloud services and deployment models will require different approaches to SLAs, adding to the complexity of SLAs. Finally, SLA terminology today often differs from one cloud service provider to another, making it difficult for cloud service customers to compare cloud services. For the avoidance of doubt, this document does not address consumers as being cloud service customers.

Standardising aspects of SLAs improves the clarity and increases the understanding of SLAs for cloud services in the market, in particular by highlighting and providing information on the concepts usually covered by SLAs.

In that context, under the second key action, the Cloud Computing Strategy calls for the development of standardisation guidelines for cloud computing service level agreements for contracts between cloud service providers and cloud service customers (not being consumers). In February 2013 the European Commission, DG CONNECT set up the Cloud Select Industry Group – Subgroup on Service Level Agreement (C-SIG-SLA) to work on this aspects. The C-SIG SLA subgroup, an industry group facilitated by the European Commission DG Connect, has prepared this document to provide a set of SLA standardisation guidelines for cloud service providers and professional cloud service customers, while ensuring the specific needs of the European cloud market and industry are taken into account.

However, this initiative will have maximum impact if standardisation of SLAs is done at an international level, rather than at a national or regional level. International standards, such as ISO/IEC 19086, provide a good venue to achieve this objective. Taking this into account, the C-SIG SLA Subgroup, as the European Commission expert group, set up a liaison with the ISO Cloud Computing Working Group[1] to provide concrete input and present the European position at the international level. The SLA Standardisation Guidelines will serve as a basis for the further work of the C-SIG SLA and for a contribution to the ISO/IEC 19086 project[2].

[1] ISO/IEC JTC 1/SC 38 - http://www.iso.org/iso/home/standards_development/list_of_iso_technical_committees/iso_technical_committee.htm?commid=601355

[2] http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=63902

1. Principles for the development of Service Level Agreement Standards for Cloud Computing

The Internet and other advances in computing have spawned a global digital economy and the continuing evolution of cloud computing has added a new and rapidly growing dynamic. While cloud computing is increasing in maturity, it is still in its nascent stages and the related technologies, business models and polices will undoubtedly evolve over a number of years.

There are a number of efforts underway to facilitate adoption of cloud computing by adding clarity to the agreements between cloud service customers and cloud service providers, thus making them more comparable and comprehensible. These efforts are valuable but at the same time it is important to not constrain the technical and business innovation of cloud computing.

The following is a set of principles that can assist organizations, through the development of standards and guidelines for cloud SLAs and other governing documents. These principles are not intended to be limiting nor to even set model terms.

1.1. Technology Neutral

Essential hallmarks of cloud computing are flexibility and extensibility for which technology neutrality is a necessary foundation.

Cloud services can be built using any number of technologies and a particular technology stack should not be assumed.

For example, many cloud services expose REST interfaces or APIs but they can also use technologies such as Web Services to receive data and interoperate with other services.

In another example being technology neutral is important because cloud services commonly run on virtualized hardware platforms but virtualization should not be assumed.

Continuous improvement to deliver increasing value is critical to the future of cloud computing and the freedom to innovate technically is key to that.

Cloud services are built on open source software and proprietary software alike. There can also be a variety of hardware platforms underlying cloud services.

1.2. Business Model Neutral

A particular business model for cloud services should not be assumed. Cloud services may be funded by any number of methods such as pay per use, long term contracts, advertising, public funds and others. Remedies for failure to achieve cloud service level objectives (SLOs) stated in the SLA can also take different forms such as refunds on charges, free services or other forms of compensation.

1.3. World-wide applicability

The Internet is a global communications channel and it is built on standards that are respected worldwide. Likewise, cloud services have a global audience of governments, small businesses, enterprises, NGOs and individuals. Agreements that govern cloud services must account for regional, national and local laws, regulations and policies but everyone benefits from globally common concepts, vocabulary and globally accessible technology.

1.4. Unambiguous definitions

Keeping the definition of service level objectives well-defined and unambiguous is important to ensure the effective standardization of cloud SLAs and to enable clear communication between cloud service providers and cloud service customers. As technology develops and new terminology is developed it will also be important to ensure definitions are up-to-date and consistent with an evolving cloud services landscape.

1.5. Comparable Service Level Objectives

Service Level objectives ('SLO') are often quantitative and have related measurements. For cloud service customers to make informed decisions when choosing cloud services, it is best if the service level objectives offered by each cloud service provider for similar services can be easily compared. Measurements should also be comparable since reduced comparability impedes adoption. However, from case to case reviewing less-quantitative or qualitative SLOs and comparing different services may provide extra insights for making such informed decision.

To be comparable, service level objectives need not be determined by identical means but sufficient information about the SLO needs to be provided by cloud service providers. Standardized terminology, metrics and templates can be helpful in documenting how a particular SLO is determined.

Service level objectives are often associated with metrics. A metric is a defined measurement method and measurement scale, which is used in relation to a quantitative service level objective.

Metrics are used to set the boundaries and margins of errors which apply to the behaviour of the cloud service and any limitations. Metrics may be used at runtime for service monitoring, balancing, or remediation. Using a standard set of metrics or metric templates in the cloud SLA makes it easier and faster to define a cloud SLA and service level objectives, and simplifies the task of comparing one cloud SLA to another.

It is often true that a given SLO may have multiple different metrics which can be used. It is important that an SLA makes it clear which metric(s) are being used for each quantitative SLO.

This document does not give a detailed description of metrics, but it is expected that common metrics for cloud SLAs will be further developed in the future[3].

1.6. Conformance through disclosure

Since standards and guidelines for cloud SLAs should be technology and business model neutral, they should not mandate a specific approach for any concept. For example, service availability can be measured in different ways[4], some of which depend on the specific cloud service. A compute service is different than a cloud email service and service availability for each will be computed differently.

Cloud service providers should document their method of achieving SLOs for each concept in their cloud SLA based on standard concepts and vocabulary.

1.7. Standards and Guidelines which span customer types

Cloud services are valuable to both enterprises with thousands of users as well as small businesses with just a few users. In many cases, the cloud service is a highly standardised offering that relies heavily on uniformity to enable economies of scale and offer customers benefits, such as low prices. In some cases, the cloud SLA and other governing documents may be negotiated between the cloud service customer and the cloud service provider but such a negotiation cannot be assumed by default. In many cases, cloud service customers are offered a fixed standard agreement by the cloud service provider, which they can either choose to accept, or they can choose a different cloud service provider that offers different terms and conditions.

Standards and guidelines for cloud SLAs must be able to span from the smallest cloud service customer to the largest. Useful standards and guidelines exist, produced by organisations such as ENISA[5], NIST[6] or ISO/IEC[7]. For example, in the field of security, relevant work is using the approach to analyze and refine an individual control into one of more security SLOs, which are then associated with metrics and measurements that can be either quantitative or qualitative.

However, it is not possible to list exhaustively relevant standards, guidelines or certifications and many other useful specification initiatives exist.

1.8. Cloud Essential Characteristics

[3] The C-SIG SLA will work on and provide input on metrics to the ISO Working Group on Cloud Computing so that it is described in generally available documents, such as the ISO 19086 standard.
[4] See ENISA report on measurements and metrics on SLAs for Cloud http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/procure-secure-a-guide-to-monitoring-of-security-service-levels-in-cloud-contracts
[5] See footnote 4
[6] NIST ."Cloud Computing: Cloud Service Metrics Description (RATAX)". Working document. 2014.
[7] ISO/IEC. "ISO/IEC 19086: Information Technology - Cloud Computing – Service Level Agreement (SLA) Framework and Terminology". Working document. ISO/IEC, 2014.

While cloud computing is a form of distributed computing, there are differences between traditional on premise and outsourced computing and cloud computing. These differences are best described in ISO/IEC 17788 'Cloud Computing Overview and Vocabulary' as[8]:

a. Broad Network Access

b. Measured Service

c. Multi-tenancy

d. On-demand self-service

e. Rapid elasticity and scalability

f. Resource pooling

While many of the concepts from traditional distributed computing SLAs apply to cloud SLAs, the specific needs of cloud computing must be recognized and accounted for.

1.9. Proof Points

Any effort to develop standards and guidelines for cloud SLAs should take into account the state-of-the-art and to some degree represent the capabilities of the cloud services industry.

The state-of-the-art should not necessarily limit the introduction of new ideas or the re-use of long standing concepts but they should be considered relative to industry's capabilities including the cloud essential characteristics. Before introducing a particular concept into a standard or guideline for cloud SLAs the organization[9] should look for proof points to ensure the concept is viable from both technical and business perspectives.

1.10. Information Rather Than Structure

Standards and guidelines for cloud SLAs should not specify the structure of the SLA, instead they should illustrate and specify the concepts that should be addressed.

What is valuable is information that helps business and technical stakeholders understand the non-legal concepts and vocabulary used in cloud SLAs.

Thus this document does not prescribe requirements that must be implemented in a service level agreement. Its main objective is to provide information that regulators, cloud service customers and providers may find helpful when considering cloud SLAs and related, sometimes overlapping, documents.

The list of SLOs in this document is not meant to be exhaustive, and it is possible that other relevant SLOs become relevant, in particular for specific sectors. Furthermore not all SLOs will be relevant for

[8] See ISO/IEC 17788 'Cloud Computing Overview and Vocabulary'. The standard will be published in the coming months.
[9] for example a standard development organisation, a cloud certification organisation, a cloud service provider or customer, etc

every cloud service: some of the concepts mentioned in this document may not be part of the standard offering for all cloud computing services, given the important differences between cloud services models (IaaS, PaaS, SaaS, xaaS), as well as the many different cloud services provided within such group of cloud services models.

The fact that an SLO is not implemented does not necessarily imply that the service is of lower quality or performing worse. There may also be cases where similar information could be derived from other SLOs.

A cloud SLA can be a part of an overall Master Service Agreement (MSA). The SLA describes and sets service level objectives for the cloud service. However, the organization and the names used for the MSA and its associated documents can vary considerably and the location of a particular service level objective within the document set can also vary. These documents may include, but are not limited to:

- Master Service Agreement (MSA)
- Service Level Agreement (SLA)
- Service Agreement
- Acceptable Use Policy
- Privacy Policy
- Security Policy
- Business Continuity Policy
- Service Description

It is important for the cloud service customer to understand the complete set of documents that govern the cloud service and to identify service level objectives wherever they occur.

1.11. Leave the Legal Agreement to Attorneys

Standards and guidelines for SLAs should specify the concepts and definitions necessary for the cloud service provider to describe the cloud service and its attributes. The agreement between the cloud service provider and cloud service customer can refer to the clearly defined information in the SLA, but the agreement itself must meet local legal requirements and those must be left to the discretion of qualified attorneys.

Furthermore, the purpose of this guideline is to inform both cloud service customers and cloud service providers about some considerations when understanding or comparing SLAs in the context of their particular situation. However, the scope of the agreed SLA may comprise some aspects which are not tackled by this document.

2. Cloud SLA Vocabulary

In this document, the following terms shall have the meaning[10] as set forth below (where the context or construction requires, all words applied in the plural shall be deemed to have been used in the singular, and vice versa).

Definition	Description
Application programming interface (API)	The collection of invocation methods and associated parameters used by a certain (part of) cloud service or software component to request actions from and otherwise interact with another cloud service or software component.
Auditability	The capability of supporting a systematic, independent and documented process for obtaining audit evidence and evaluating it objectively to determine the extent to which audit criteria are fulfilled.
Availability	The property of being accessible and usable upon demand by an authorized entity.
Cloud computing	A paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand.[11] Examples of resources include servers, operating systems, networks, software, applications, and storage equipment.
Cloud infrastructure	The collection of hardware, software and other related goods and resources that enables the provision of cloud services.
Cloud service	One or more capabilities offered via cloud computing invoked using a defined interface.
Cloud service customer	A party which is in a business relationship for the purpose of using cloud services, for this document not being consumers. NOTE – A business relationship may not necessarily imply financial agreements or similar arrangements.
Cloud service customer data	class of data objects under the control, by legal or other reasons, of the cloud service customer that were input to the cloud service, or resulted from exercising the capabilities of the cloud service by or on behalf of the

[10] The vocabulary definitions below are meant to be aligned with those in ISO/IEC 17788 http://www.iso.org/iso/catalogue_detail.htm?csnumber=60544
However this standard has not been published yet. It is expected to be published in the coming months.

[11] Cloud computing can be composed of (A) five essential characteristics being (i) on-demand self-service, (ii) broad network access, (iii) resource pooling, (iv) rapid elasticity, and (v) measured service, (B) four service models, being (i) SaaS, (ii) PaaS, (iii) IaaS, and (iv) other XaaS, and (C) four deployment models, being (i) private cloud, (ii) community cloud, (iii) public cloud, and (iv) hybrid cloud.

	cloud service customer via the published interface of the cloud service An example of legal controls is copyright.
Cloud service derived data	class of data objects under cloud service provider control that are derived as a result of interaction with the cloud service by the cloud service customer Cloud service derived data includes log data containing records of who used the service, at what times, which functions, types of data involved and so on. It can also include information about the numbers of authorized users and their identities. It can also include any configuration or customization data, where the cloud service has such configuration and customization capabilities.
Cloud service level objective (SLO)	Target for a given attribute of a cloud service that can be expressed quantitatively or qualitatively.
Cloud service provider (CSP)	A party which makes cloud services available.
Cloud service provider data	class of data objects, specific to the operation of the cloud service, under the control of the cloud service provider Cloud service provider data includes but is not limited to resource configuration and utilization information, cloud service specific virtual machine, storage and network resource allocations, overall data centre configuration and utilization, physical and virtual resource failure rates, operational costs and so on.
Cloud service user	natural person, or entity acting on their behalf, associated with a cloud service customer that uses cloud services Examples of such entities include devices and applications.
Cloud SLA life cycle	Service level agreements life cycle i.e.; assessment, negotiation, contracting, operation, amendment, escalation and termination, and other arrangements and matters.
Cloud SLAs	Documented agreement between the cloud service provider and cloud service customer that identifies services and cloud service level objectives (SLOs).
Cryptographic key management	Key management is the management of cryptographic keys in a cryptosystem. This includes dealing with the generation, exchange, storage, use, and replacement of keys, as well as cryptographic protocol. It includes cryptographic protocol design, key servers, user procedures, and other relevant protocols[12].
Data	Data of any form, nature or structure, that can be created, uploaded, inserted in, collected or derived from or with cloud services and/or cloud

[12] http://en.wikipedia.org/wiki/Key_management

	computing, including without limitation proprietary and non-proprietary data, confidential and non-confidential data, non-personal and personal data, as well as other human readable or machine readable data.
Data controller	The natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data.
Data format	One or more formats in which the data is in one or more phases of its data lifecycle.
Data integrity	The property of protecting the accuracy and completeness of assets.
Data intervenability	The capability of a cloud service provider to support the cloud service customer in facilitating exercise of data subjects' rights. Note: Data subjects' rights include without limitation access, rectification, erasure of the data subjects' personal data. They also include the objection to processing of the personal data when it is not carried out in compliance with the applicable legal requirements.
Data life cycle	The handling of data that commonly includes six (6) phases, (1) create/derive, (2) store, (3) use/process, (4) share, (5) archive, (6) destroy.[13]
Data location	The geographic location(s) where personal data may be stored or otherwise processed by the cloud service provider.
Data portability	Ability to easily transfer data from one system to another without being required to re-enter data.
Data processor	A natural or legal person, public authority, agency or any other body which processes Personal data on behalf of the Data controller.
Data protection	The employment of technical, organisational and legal measures in order to achieve the goals of data security (confidentiality, integrity and availability), transparency, intervenability and portability, as well as compliance with the relevant legal framework.
Data subject	An identified or identifiable natural person, being an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.
Hybrid cloud	Deployment model of cloud computing using at least two different cloud deployment models.
Identity assurance	The ability of a relying party to determine, with some level of certainty, that a claim to a particular identity made by some entity can be trusted to actually be the claimant's true, accurate and correct identity.
Incident notification and transparency	Notifications and transparency about incidents under the SLA that may be required as per (a) mandatory law and legislation (such as under the EU

[13] https://cloudsecurityalliance.org/download/security-guidance-for-critical-areas-of-focus-in-cloud-computing-v3/

	Network and Information Security ('NIS') Directive), and/or (b) contractual arrangement.
Information security	The preservation of confidentiality, integrity and availability of information.
Infrastructure as a service (IaaS)	The capability provided to the cloud service customer is to provision processing, storage, networks, and other fundamental computing resources where the cloud service customer is able to deploy and run arbitrary software, which can include operating systems and applications. The cloud service customer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).
Incident management	The processes for detecting, reporting, assessing, responding to, dealing with, and learning from information security incidents.
Metric	A metric is a defined measurement method and measurement scale, which is used in relation to a quantitative service level objective.
Personal data	Any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.
Platform as a service (PaaS)	The capability provided to the cloud service customer is to deploy onto the cloud infrastructure customer-created or acquired applications created using programming languages, libraries, services, and tools supported by the CSP. The cloud service customer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed.
Private cloud	The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple cloud service customers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.
Processing of personal data	Any operation or set of operations which is performed upon Personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.
Public cloud	The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the CSP and/or its suppliers.
Response time	Time interval between a cloud service customer initiated event (stimulus) and a cloud service provider initiated event in response to that stimulus.

REST	Representational state transfer (REST) is a software architectural style consisting of a coordinated set of architectural constraints applied to components, connectors, and data elements, within a distributed hypermedia system.
Reversibility	Process for cloud service customers to retrieve their cloud service customer data and application artefacts and for the cloud service provider to delete all cloud service customer data as well as contractually specified cloud service derived data after an agreed period.
Sensitive data	Any classified, personal, proprietary or confidential information or data of any form, nature or structure, that can be created, uploaded, inserted in, collected or derived from or with cloud services and/or cloud computing whose access, use, disclosure or processing is subject to restriction either by applicable law or contact.[14]
Software as a services *(SaaS)*	The capability provided to the cloud service customer is to use the cloud service provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g. web-based email), or a program interface. The cloud service customer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.
Temporary data	Data or a data set that is created during the operation of the cloud service and becomes unused after a predefined period of time.
Vulnerability	A weakness of an asset or group of assets, e.g. software or hardware related, that can be exploited by one or more threats.
xaaS	A collective term of diverse but re-useable components, including without limitation infrastructure, platforms, data, software, middleware, hardware or other goods, made available as a service with some kind of use of cloud computing.

[14] This includes (but is not limited to) sensitive data pursuant to the 95/46/EC directive for the protection of personal data, for which the definition of the directive applies.

3. Performance Service Level Objectives Overview

This section covers the common service level objectives that relate to the performance of the cloud service and the performance of related aspects of the interface between the cloud service customer and the cloud service provider. The set of service level objectives is not exhaustive, but not all the service level objectives are applicable to all cloud services.

3.1. Availability

Description of the context or of the requirement

Availability is the property of being accessible and usable upon demand by an authorized entity.

Description of the need for SLOs, in addition to information available through certification

Availability is usually covered by certification at a general level. Availability is a key service level objective, since it describes whether the cloud service can actually be used, and it is typically necessary to specify numeric values for availability to make meaningful statements that are useful for cloud service customers.

The question of what "usable" means is a complex matter, which depends on the cloud service concerned. A service can be up and available, but perform so poorly that it is effectively unusable. Similarly, the service can be up, but respond with errors for valid requests. It can be valuable for the SLA to provide clear information on these aspects of service availability.

Description of relevant SLOs

Level of uptime (Often termed "availability")	describes the time in a defined period the service was available, over the total possible available time, expressed as a percentage.[15] Some cloud services specify that the service will be unavailable for specified periods for maintenance. It is common for the stated level of uptime to exclude these maintenance periods. In this case Uptime = Total Possible Available Time – (Total Downtime – Maintenance Downtime).
Percentage of successful requests	describes the number of requests processed by the service without an error over the total number of submitted requests, expressed as a percentage.
Percentage of timely service provisioning requests	describes the number of service provisioning requests completed within a defined time period over the total number of service provisioning requests, expressed as a percentage. Provisioning of cloud services may vary greatly depending on the type of

[15] Uptime can be defined as the Total Possible Available Time – (Downtime – Allowable Downtime). The Total Possible Available Time is the number of total minutes, hours, seconds in the measurement period, usually a billing month. Allowable Downtime accounts for scheduled maintainance and any other element carved out in the agreement

	service being considered – from storage provisioning to user account provisioning. It is thus expected that this SLO will need to be tailored to the particular service being considered.

3.2. Response Time

Description of the context or of the requirement

Response time is the time interval between a cloud service customer initiated event (stimulus) and a cloud service provider initiated event in response to that stimulus. The response time SLOs can vary depending on the point at which the customer stimulus is measured. For example, the measurement may start from when the customer initiates the stimulus on their device, or it may start from the point where when the request from the customer arrives at the cloud service provider's endpoint – the difference being the network transit time, which may be outside the control of the cloud service provider. Similarly, the point at which the response is measured can vary.

Description of the need for SLOs, in addition to information available through certification

Response time can be a highly significant aspect of the user experience of a cloud service – for some requests, response times that are greater than some threshold are regarded as unacceptable and can make the cloud service effectively unusable. Rarely are response times dealt with directly by certifications and furthermore, response times can vary depending on the nature of the request concerned or the type of the service being considered.

A factor that needs to be considered is that many cloud services support multiple different operations and that it is likely that the response time will differ for the different operations. As a result, response time SLOs need to clearly state which operation(s) are concerned.

Description of relevant SLOs

Average response time	refers to the statistical mean over a set of cloud service response time observations for a particular form of request.
Maximum response time	refers to the maximum response time target for a given particular form of request.

3.3. Capacity

Description of the context or of the requirement

Capacity is the maximum amount of some property of a cloud service. It is often an important value for cloud service customers to know when using a cloud service.
The relevant properties vary depending on the capabilities offered by the cloud service and it is often the case that multiple different capacities are relevant for a given cloud service.

Description of the need for SLOs, in addition to information available through certification

Capacities are rarely the subject of certification and must be stated clearly in the SLA for a cloud service. Note that capacity SLOs refer to the capacities as seen by an individual cloud service customer and do not reflect the overall capacities supported by the cloud service provider – indeed it

is commonly the case that the customer can change the capacity limits for their cloud service(s) by requesting a change in their subscription.

Description of relevant SLOs

There are a number of SLOs, which relate to the capacity of a cloud service

Number of simultaneous connections	refers to the maximum number of separate connections to the cloud service at one time.
Number of simultaneous cloud service users	refers to a target for the maximum number of separate cloud service customer users that can be using the cloud service at one time.
Maximum resource capacity	refers to the maximum amount of a given resource available to an instance of the cloud service for a particular cloud service customer. Example resources include data storage, memory, number of CPU cores.
Service Throughput	refers to the minimum number of specified requests that can be processed by the cloud service in a stated time period. (e.g. Requests per minute).

3.4. Capability Indicators

Description of the context or of the requirement

Capability indicators are service level objectives which promise specific functionality relating to the cloud service.

Description of the need for SLOs, in addition to information available through certification

Capabilities can be essential to the use of the cloud service from the perspective of the cloud service customer.

Description of relevant SLOs

External connectivity	specifies capabilities of the cloud service to connect to systems and services which are external to the cloud service. The systems and services involved may be other cloud services or they may be outside cloud computing (e.g. in-house customer systems).

3.5. Support

Description of the context or of the requirement

Support is an interface made available by the cloud service provider to handle issues and queries raised by the cloud service customer.

Description of the need for SLOs, in addition to information available through certification

Support capabilities may be required by certification, but the details are typically not covered by certification and must instead be described by SLOs.

Description of relevant SLOs

Support hours	specifies the hours during which the cloud service provider provides a cloud service customer support interface that accepts general inquiries and requests from the cloud service customer.
Support responsiveness	specifies the maximum time the cloud service provider will take to acknowledge a cloud service customer inquiry or request. It is typical for responsiveness to vary depending on a severity level which is attached to the customer request, with a shorter response time associated with higher severity levels.[16]
Resolution time	refers to the target resolution time for customer requests – in other words, the time taken to complete any necessary actions as a result of the request. This target time can vary depending on the severity level of the customer request, with shorter times attached to requests of higher severity.

3.6. Reversibility and the Termination Process

Description of the context or of the requirement

The termination process takes place when a cloud service customer or a cloud service provider elect to terminate the agreement. The termination process includes a series of steps which enable the customer to retrieve their cloud service customer data within a stated period of time before the cloud service provider deletes the cloud service customer data from the provider's systems (including backup copies, which may be done possibly on a different schedule). The cloud service provider can potentially delete or aggregate any cloud service derived data (this is limited to derived data related to operations) that relates to the customer and their use of the cloud service, although such deletion may be limited in scope.

Description of the need for SLOs, in addition to information available through certification

Certification may require a well defined termination process but does not typically define aspects such as the time periods involved.

Description of relevant SLOs

Data retrieval period	specifies the length of time in which the customer can retrieve a copy of their cloud service customer data from the cloud service.
Data retention period	refers to the length of time which the cloud service provider will retain backup copies of the cloud service customer data during the termination process (in case of problems with the retrieval process or for legal

[16] Support responsiveness does not necessarily take into account the time for closing the request, which may vary based on the specific circumstances.

	purposes). This period may be subject to legal or regulatory requirements, which can place lower or upper bounds on the length of time that the provider can retain copies of cloud service customer data.
Residual data retention	refers to a description of any data relating to the cloud service customer which is retained after the end of the termination process – typically this will be cloud service derived data, which could be subject to regulatory controls.

4. Security Service Level Objectives Overview

Specifying measurable security level objectives in SLAs is useful to improve both assurance and transparency. At the same time, it allows for establishing a common semantics in order to manage cloud security from two perspectives, namely (i) the security level being offered by a cloud service provider and, (ii) the security level requested by a cloud service customer.

The approach used in this section consists of analysing security controls from well-known frameworks[17] into one or more security SLOs, when appropriate. These SLOs can be either quantitative or qualitative. This section focuses on the definition of possible security SLOs. Eight categories are provided, each with one or more SLOs.

The categories are representative of some important security requirements. However not all security requirement categories are reflected below, as relevant SLOs may not exist for each of them. For example resilience, business continuity and disaster recovery are important aspects of security, specific controls and measures are usually put in place by CSPs, but no SLO has been derived for these security aspects.

For each category, the SLOs are meant to provide more quantitative and qualitative information relevant to a specific control, in addition to what is usually assessed in the context of an audit for a certification (please also refer to Section 1.7).

It should be noted that the list of SLOs is not meant to be considered as exhaustive and that the SLOs proposed are not meant to be considered as applicable in all individual cases. The applicability of a particular SLO can depend on the type of service offered (in terms of both of service functionally and service model) and pricing of it (free service, paid, premium). It is important to understand that some of the SLOs relevant to security also have relevance in the areas of Data Management, Performance and Data Privacy and those SLOs are found in those sections.

4.1. Service Reliability

Description of the context or of the requirement

Service reliability is the property of a cloud service to perform its function correctly and without failure, typically over some period of time. This category is usually related to the security controls implementing business continuity management and disaster recovery in frameworks like ISO/IEC 27002 (cf. footnote 17). Allowable downtime, which accounts for scheduled maintenance and any other element carved out in the agreement, should be taken into account for this SLO.

Note that reliability also covers the capability of the cloud service to deal with failures and to avoid loss of service or loss of data in the face of such failures.

Description of the need for SLOs, in addition to information available through certification

[17] Relevant security frameworks include in particular ISO/IEC 27001 and ISO/IEC 27002

Reliability is sometimes covered by certification, but the target for reliability needs to be stated so that the cloud service customer can assess whether the particular cloud service meets their business requirements. Some data management SLOs can be relevant to reliability – see section 5 on data management SLOs.

Description of relevant SLOs

Level of redundancy	describes the level of redundancy of the cloud service supply chain, possibly taking into account the percentage of the components or service that have fail over mechanism. Redundancy varies also on the type of cloud service provided (IaaS versus SaaS for example)).
Service reliability	describes the ability of the cloud service to perform its function correctly and without failure over some specified period.

4.2. Authentication & Authorization

Description of the context or of the requirement

Authentication is the verification of the claimed identity of an entity (typically for cloud computing the entity is a cloud service user).
Authorization is the process of verifying that an entity has permission to access and use a particular resource based on predefined user privileges.

Authentication and authorization are key elements of information security which apply to the use of cloud services.

Description of the need for SLOs, in addition to information available through certification

Certification generally validates that authentication and authorization mechanisms are in place for a system, but do not in general provide details of how those mechanisms are provided, which can be essential information for the cloud service customer.

Description of relevant SLOs

User authentication and identity assurance level	measures the Level of Assurance (LoA) of the mechanism used to authenticate a user accessing a resource. The LoA can be based on relevant standards like NIST SP 800-63 (Electronic Authentication Guidelines), ISO/IEC 29115 (Entity Authentication Assurance Framework) or the Kantara Initiative's Identity Assurance Framework (IAF).
Authentication	specifies the available authentication mechanisms supported by the CSP on its offered cloud services. In some cases the customer might need to analyse along with the CSP, those mechanisms allowing interoperability among their authentication schemes (e.g., cross-certification in the case of digital certificate-based

	authentication).
Mean time required to revoke user access	is the arithmetic average of the times required to revoke users' access to the cloud service on request over a specified period of time.
User access storage protection	describes the mechanisms used to protect cloud service user access credentials
Third party authentication support	specifies whether third party authentication is supported by the cloud service and defines which technologies can be used for third party authentication[18]. This SLO complements the previously defined "Authentication", and is the basis for interoperable authentication/identity management solutions between customer and providers.

4.3. Cryptography

Description of the context or of the requirement

Cryptography is a discipline which embodies principles, means and methods for the transformation of data in order to hide its information content, prevent its undetected modification and/or prevent its unauthorized use. Also known by the term encryption.

Description of the need for SLOs, in addition to information available through certification

While many certification approaches require the use of data encryption in a variety of circumstances, there are many encryption methods in use and these methods vary in their strength and also vary in their cost - either in terms of performance or of the necessary processing power to use them. It is necessary for the SLA to describe specifics relating to encryption methods in order for the cloud service customer to evaluate a cloud service fully, since few certifications require the use of specific encryption methods.

Description of relevant SLOs

Cryptographic brute force resistance	expresses the strength of a cryptographic protection applied to a resource based on its key length, for example using the ECRYPT II security level recommendations [19] or the FIPS security levels[20] for encryption. Instead of using key lengths alone, which are not always directly comparable from one algorithm to another, this normalizing scale allows comparison of the strengths of different types of cryptographic algorithms.
Key access control policy	describes how strongly a cryptographic key is protected from access, when it is used to provide security to the cloud service (or assets within the cloud service).
Cryptographic hardware module	describes the level of protection that is afforded to cryptographic operations in the cloud service through the use of cryptographic hardware

[18] Other authentication SLOs may become less relevant if authentication if performed by a 3rd party.
[19] Smart N. (ed.). "ECRYPT II Yearly Report on Algorithms and Keysizes (2010-2011)". Katholieke Universiteit Leuven (KUL). Deliverable SPA-17. rob June, 2011. Online: http://www.ecrypt.eu.org/documents/D.SPA.17.pdf
[20] http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

protection level	modules.

4.4. Security Incident management and reporting

Description of the context or of the requirement

An information security incident is a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security. Information security incident management are the processes for detecting, reporting, assessing, responding to, dealing with, and learning from information security incidents.

Description of the need for SLOs, in addition to information available through certification

How information security incidents are handled by a cloud service provider is of great concern to cloud service customers, since an information security incident relating to the cloud service is also an information security incident for the cloud service customer.

Description of relevant SLOs

Percentage of timely incident reports	describes the defined incidents to the cloud service which are reported to the customer in a timely fashion. This is represented as a percentage by the number of defined incidents reported within a predefined time limit after discovery, over the total number of defined incidents to the cloud service which are reported within a predefined period (i.e. month, week, year, etc).
Percentage of timely incident responses	describes the defined incidents that are assessed and acknowledged by the cloud service provider in a timely fashion. This is represented as a percentage by the number of defined incidents assessed and acknowledged by the cloud service provider within a predefined time limit after discovery, over the total number of defined incidents to the cloud service within a predefined period. (iei.e. month, week, year, etc)).
Percentage of timely incident resolutions	describes the percentage of defined incidents against the cloud service that are resolved within a predefined time limit after discovery.

4.5. Logging and Monitoring

Description of the context or of the requirement

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.

Description of the need for SLOs, in addition to information available through certification

Log file entries are important to cloud service customers when analysing incidents such as security breaches and service failures as well as in monitoring the customer's day-to-day use of the service. It is necessary for there to be service level objective relating to logging and monitoring in order to fully describe the cloud service and its related capabilities.

Description of relevant SLOs

Logging parameters	describes the parameters that are captured in the cloud service log files .
Log access availability	describes what log file entries the cloud service customer has access to.
Logs retention period	describes the period of time during which logs are available for analysis (e.g. the period of time that log files are available for use by the cloud service customer)).

4.6. Auditing and security verification

Description of the context or of the requirement

Auditing is the systematic, independent and documented process for obtaining audit evidence about a cloud service and evaluating it objectively to determine the extent to which the audit criteria are fulfilled. The audit evidence required and the audit criteria are usually determined by the audit scheme or certification scheme which is used to perform the audit. Certification is one of many ways to address audits.

Description of the need for SLOs, in addition to information available through certification

Audits are a means by which the cloud service provider can offer independent evidence that a cloud service meets particular criteria of interest to the cloud service customer – aiming to increase trust in the cloud service.

Description of relevant SLOs

Certifications applicable	refers to a list of certifications held by the cloud service provider for a cloud service, including the certifying body, the expiration date of each certification and the renewal period[21].

4.7. Vulnerability Management

Description of the context or of the requirement

A vulnerability is a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat.

[21] See for example ENISA's Cloud Computing Certification Schemes List (https://resilience.enisa.europa.eu/cloud-computing-certification)

Management of vulnerabilities means that information about technical vulnerabilities of information systems being used should be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.

Description of the need for SLOs, in addition to information available through certification

Many of the information systems associated with a cloud service belong to the cloud service provider with the result that the cloud service customer is dependent on the provider for appropriate and timely management of vulnerabilities of those systems. SLOs for vulnerability management provide transparency for the customer.

Description of relevant SLOs

Percentage of timely vulnerability corrections	describes the number of vulnerability corrections performed by the cloud service provider, and is represented as a percentage by the number of vulnerability corrections performed within a predefined time limit, over the total number of vulnerability corrections to the cloud service which are reported within a predefined period (i.e. month, week, year, etc).
Percentage of timely vulnerability reports	describes the number of vulnerability reports by the cloud service provider to the cloud service customer, and is represented as a percentage by the number of vulnerability reports within a predefined time limit, over the total number of vulnerability reports to the cloud service which are reported within a predefined period (i.e. month, week, year, etc).
Reports of vulnerability corrections	is a description of the mechanism by which the cloud service provider informs the customer of vulnerability corrections applied to the provider's systems, including the frequency of the reports.

4.8. Governance

Governance is system by which cloud service is directed and controlled. The main area of concern is the way in which changes and updates to a cloud service are managed, whether the change request originates with the cloud service customer or originates with the cloud service provider.

4.8.1. Service changes

Description of the context or of the requirement

Cloud services may change from time to time. Examples of service changes include changes to functionality, changes to the service's interfaces and the application of software updates.
Change to a particular service can be reflected in the SLA or in another contractual document.

Description of the need for SLOs, in addition to information available through certification

Cloud service customers need a reasonable notification period before changes to a cloud service take effect so that they can plan appropriately.

Description of relevant SLOs

Cloud service change	describes the type of change (such as SLA change or functional change),

reporting notifications	mechanism and period for the cloud service provider to notify cloud service customers of planned changes to the cloud service.
Percentage of timely cloud service change notifications	The number of change notifications made within a specified period of time over the total number of change notifications, expressed as a percentage.

5. Data Management Service Level Objectives Overview

As companies transition to cloud computing, the traditional methods of securing and managing data are challenged by cloud-based architectures. Elasticity, multi-tenancy, new physical and logical architectures, and abstracted controls require new data security strategies. Managing data and information in the era of cloud computing can affect all organizations. It begins with managing internal data and cloud migrations and extends to securing information in diffuse, cross-organization applications and services.

The data management SLOs presented in this section cope with important quantitative and qualitative indicators related with data life cycle management, and can be considered as complementary to existing and applicable security and data protection certifications offered by the cloud service provider.

Presented data management SLOs are subdivided in four (4) different top-level categories covering all aspects of the identified data life-cycle. Each category is subdivided in one of more SLOs that are applicable to that specific category. Not all SLOs may be relevant for each cloud service, in particular depending on the type of cloud service such as IaaS, PaaS or SaaS.

5.1. Data classification

Description of the context or of the requirement

Data classification is a description of the classes of data which are associated with the cloud service:

- cloud service customer data
- cloud service provider data
- cloud service derived data

Cloud service customer data is a class of data objects under the control of the cloud service customer. Cloud service customer data includes data input into the cloud service by the cloud service customer and the results of the cloud service customer's use of the cloud service, unless the master service agreement specifically defines a different scope.

Description of the need for SLOs, in addition to information available through certification

The following SLOs contain a specific list of data uses (provider and derived), that can be applied to compare different CSP offers in a concrete manner. This information is usually difficult to deduce in such a specific and concrete way from relevant security/data protection certifications. Customers should use this information to make informed decisions about their choice of CSP – e.g. are the CSP's listed "customer data uses" compliant with my requirements?

Description of relevant SLOs

Cloud service customer data use by the provider	describes stated policy for any intended use of cloud service customer data
Cloud service	describes what derived data is created by the cloud service provider from

derived data use	cloud service customer data, the intended uses for the derived data and what rights the cloud service customer has to inspect the derived data

5.2. Cloud Service Customer Data Mirroring, Backup & Restore

Description of the context or of the requirement

This SLO category deals with the actual mechanisms used to guarantee that the customers' data is available (online or offline) in case of failures forbidding access to it. The mechanisms falling under the scope of this SLO are divided in two widely-used categories (i) data mirroring, (ii) backup/restore.

Description of the need for SLOs, in addition to information available through certification

Widely used security certification[22] contains specific security controls that are implemented to avoid data loss[23]. However, in many cases the information that can be extracted from those certifications rarely contains the basic measurements that can be used by the cloud service customer to assess/monitor if the implemented data security controls actually fulfil her requirements. In particular with refer to SLOs in the following areas:

- The timeliness of the mirroring mechanisms, which might be directly related with the geographical location of the cloud service provider's data centres,
- Concrete details related with to the frequency and method used by the cloud service provider's backup and recovery mechanism(s).

Proposed SLOs allow customers e.g., to fine-tune their risk assessment and business continuity procedures.

The SLOs can assist the cloud service customer in putting in place Recovery Point Objective and Recovery Time Objective when using the cloud service.

Recovery Point Objective is the maximum allowable time between recovery points. RPO does not specify the amount of acceptable data loss, only the acceptable time window. In particular, RPO affects data redundancy and backup. A small RPO suggests mirrored storage of both transient and persistent data while a larger window allows for a periodic backup approach. As with RTO, cloud service customers should determine their acceptable RPO for each cloud service they use and ensure that the cloud service provider's and their own disaster recovery plans meet their objectives.

Recovery Time Objective is the maximum amount of time a business process may be disrupted, after a disaster, without suffering unacceptable business consequences. Cloud services can be critical components of business processes. Cloud service customers must determine the RTO for each of their cloud service dependent business processes and likewise determine whether the cloud service provider's and the cloud service customer's disaster recovery plans are sufficient

Description of relevant SLOs

Data Mirroring	refers to the difference between the time data is placed on primary

[22] e.g. ISO/IEC 27002, see ENISA list of cloud certifications in footnote 21
[23] e.g. "Operations Security – Backup" in ISO/IEC 27002

Latency	storage and the time the same data is placed on mirrored storage.
Data Backup Method	refers to a list of method(s) used to backup cloud service customer data.
Data Backup Frequency	refers to the period of time between complete backups of cloud service customer data.
Backup Retention Time	refers to the period of time a given backup is available for use in data restoration .
Backup Generations	refers to the number of backup generations available for use in data restoration.
Maximum Data Restoration time	refers to the committed time taken to restore cloud service customer data from a backup.
Percentage of Successful Data Restorations	refers to the committed success rate for data restorations, expressed as the number of data restorations performed for the customer without errors over the total number of data restorations, expressed as a percentage.

5.3. Data Lifecycle

Description of the context or of the requirement

The following list of SLOs is related with the efficiency and effectiveness of the provider's data-life cycle practices, with a particular focus on the practices and mechanisms for data handling and deletion.

Description of the need for SLOs, in addition to information available through certification

Despite widely-used security certifications schemes usually deal with the topic of secure disposal[24] usually the CSP-specific information related with the deletion and storage controls is not easy to extract. On one hand, the following list of SLOs provides information related with the assurance and timeliness associated with the deletion mechanism. On the other hand, are also presented quantitative SLOs associated with the reliability of the storage service (data retrievability and stored data's durability). Furthermore it may be of interest for the cloud service customer to be able to retrieve data after a deletion request has been posted and to have SLOs associated with that.
Cloud service customers are expected to use the following list of SLOs to e.g., decide on the choice of available cloud storage mechanisms offered by the CSP.

Description of relevant SLOs

Data deletion type	describes the quality of data deletion, ranging from 'weak' deletion where only the reference to the data is removed, to 'strong' sanitization techniques to ensure that deleted data cannot be easily recovered[25].
Percentage of timely effective deletions	refers to the number of cloud service customer data deletion requests completed within a predefined time limit over the total number of deletion requests, expressed as a percentage.
Percentage of tested storage retrievability	refers to the amount of cloud service customer data that has been verified to be retrievable during the measurement period, after the data has been

[24] e.g., "Data Security & Information Lifecycle Management" in CSA's Cloud Controls Matrix
[25] For more information on this topic please refer to "NIST Special Publication 800-88: Guidelines for Media Sanitization".

	deleted.

5.4. Data Portability

Description of the context or of the requirement

The following list of SLOs is related with the CSP capabilities to export data, so it can still be used by the customer e.g., in the event of terminating the contract.

Description of the need for SLOs, in addition to information available through certification

In related security controls frameworks and certifications the implementation of data portability controls usually focuses on the specification of applicable CSP policies, which makes it difficult (and sometimes impossible) for cloud service customers to extract the specific indicators related with available formats, interfaces and transfer rates. The following list of SLOs focuses on these three basic aspects of the CSP data portability features, which can be used by the customer e.g., to negotiate the technical features associated with the provider's termination process.

Description of relevant SLOs

Data portability format	specifies the electronic format(s) in which cloud service customer data can be transferred to/accessed from the cloud service.
Data portability interface	specifies the mechanisms which can be used to transfer cloud service customer data to and from the cloud service. This specification potentially includes the specification of transport protocols and the specification of APIs or of any other mechanism that is supported.
Data transfer rate	refers to the minimum rate at which cloud service customer data can be transferred to/from the cloud service using the mechanism(s) stated in the data interface.

6. Personal Data Protection Service Level Objectives Overview

This paragraph focuses on the definition of appropriate SLOs with reference to the cases where the cloud service provider acts as a data processor, on behalf of its customer (data controller), which typically applies to B2B services[26]. Providers that act as data controllers or joint controllers (notably by processing personal data for their own purposes, outside of an explicit mandate from the customer) may still make reference to this document, but they and their customers need to ensure compliance with legal obligations that may derive from their controller role.

Besides, this paragraph concentrates on data protection measures that are suitable for being translated into SLOs, i.e. into objectives that must be achieved by the provider. Other data protection measures and obligations can be better managed through other instruments, such as adherence to a code of conduct, certification against an approved standard and the relevant contract and/or service agreement and applicable law.

In this context, it should be mentioned that there is on-going initiative of the C-SIG Code of Conduct Subgroup on the Data Protection Code of Conduct for cloud service providers[27]. In order to align both initiatives, this paragraph of the SLA Standardization Guidelines will be revised and updated after receiving the approval of the final version of the Code from the Article 29 Working Party.

6.1. Codes of conduct, standards and certification mechanisms

Description of the context of the requirement

The cloud service customer, as data controller, must accept responsibility for abiding by the applicable data protection legislation. Notably, the cloud service customer has an obligation to assess the lawfulness of the processing of personal data in the cloud and to select a cloud service provider that facilitates compliance with the applicable legislation.

In this regard, the cloud service provider should make available all the necessary information, also in adherence to the principle of transparency, as described hereinafter. Such information includes information that may assist in the assessment of the service, such as the data protection codes of conduct, standards or certification schemes that the service complies with.

Description of the need for SLOs, in addition to information available through certification, adherence to codes of conduct, etc.

[26] The cloud costumer determines the ultimate purposes of the processing of (personal) data and, notably, decides to entrust such processing to the cloud service provider; the cloud customer therefore acts as data controller. When the cloud service provider supplies the means and the platform for such processing, acting on behalf of the cloud customer, the provider is considered as a data processor. (In fact, according to Dir. 95/46/EC, the data controller is the natural or legal person, public authority or any other body that determines the purposes and means of the processing of personal data; the data processor is the natural or legal person, public authority or any other body that processes personal data on behalf of the controller).

[27] The Code of Conduct has been prepared by the Cloud Select Industry Group (C-SIG) – Data Protection Code of Conduct Subgroup and has been submitted to the Article 29 Working Party for positive opinion. The work on the Code has been coordinated by the European Commission (DG Justice and DG Connect) https://ec.europa.eu/digital-agenda/en/cloud-select-industry-group-code-conduct

In the context of the above mentioned obligations, the information indicated hereinafter is useful in order to let the customer assess the cloud service's level of compliance with the applicable regulatory framework[28].

Description of relevant SLOs

Applicable data protection codes of conduct, standards, certifications	A list of the data protection codes of conduct, standards and certification mechanisms that the service complies with.[29]

6.2. Purpose specification

Description of the context of the requirement

The principle of purpose specification and limitation requires that personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes[30]. Therefore, the purposes of the processing must be determined, prior to the collection of personal data, by the data controller, who must also inform the data subject thereof.
When the data controller decides to process the data in the cloud, it must be ensured that personal data are not (illegally) processed for further purposes by the cloud service provider, or one of his subcontractors.

Description of the need for SLOs, in addition to information available through certification, adherence to codes of conduct, etc.

In general, the cloud service provider may not process personal data, pursuant to the service agreement with its customer, for its own purposes, without the express permission of the customer. Otherwise, a cloud service provider that process the customers' personal data for its own purposes outside of an explicit mandate from its customers (e.g. in order to do market analysis or scientific analysis, to profile data subjects, or to improve direct marketing, all for its own account), will qualify as a data controller in its own right and must fulfil all the relevant obligations.

It is therefore important that the list of processing purposes (if any), which are beyond those requested by the customer, is defined.

Description of relevant SLOs

Processing purposes	A list of processing purposes (if any) which are beyond those requested by the customer acting as a controller.[31]

[28] Some of these aspects were explained in details in the above mentioned Code of Conduct.
[29] This may include the above mentioned EU Data Protection Code of Conduct for Cloud Service Providers, ISO/IEC 27018, an international standard for the processing of personal data in the cloud, etc.
[30] Cf. Article 6(b) of Directive 95/46/EC
[31] It is possible that there is no processing purposes which are beyond those requested by the customer acting as a controller. Furthermore the cloud service customer can itself be a cloud service processor.

6.3. Data minimization

Description of the context of the requirement

The cloud service customer is responsible for ensuring that personal data are erased (by the provider and any subcontractors) from wherever they are stored as soon as they are no longer necessary for the specific purposes.
Furthermore temporary data can be created during the operation of the cloud service, and may not be immediately deleted once they become unused for technical reasons. Periodic checks should ensure that such temporary data is effectively deleted after a predefined period.

Description of the need for SLOs, in addition to information available through certification, adherence to codes of conduct, etc.

The contract between the cloud service customer and the provider must include clear provisions for the erasure of personal data[32]. Furthermore, since personal data may be kept redundantly on different servers at different locations, it must be ensured that each instance of them is erased irretrievably (i.e., previous versions, temporary files, etc.).
The following SLOs complement these indications, by translating them in a measurable objective that applies the data minimization principle in the course of the service.

Description of relevant SLOs

Temporary data retention period	The maximum period of time that temporary data is retained after identification that the temporary data is unused.
Cloud service customer data retention period	The maximum period of time that cloud service customer data is retained before destruction by the cloud service provider and after acknowledgment of a request to delete the data or termination of the contract.

6.4. Use, retention and disclosure limitation

Description of the context of the requirement

The cloud service provider, in its capacity as data processor, should inform the customer, in the most expedient time possible under the circumstances, of any legally binding request for which the provider is compelled to disclose the personal data by a law enforcement or governmental authority, unless otherwise prohibited, such as a legal prohibition to preserve the confidentiality of an investigation.

Description of the need for SLOs, in addition to information available through certification, adherence to codes of conduct, etc.

Besides the above mentioned obligation to inform the customer, the following SLOs aims to quantify the disclosures to law enforcement authorities over a period of time; this may also permit the customer to compare multiple offerings by different providers.

[32] Cf. Article 29 Working Party Opinion no. 5/2012 on cloud computing (hereinafter the "WP 29 Opinion")

Description of relevant SLOs

Number of customer data law enforcement disclosures	refers to the number of personal data disclosures to law enforcement authorities over a predefined period of time (applicable only if the communication of such disclosures is permitted by law).
Number of personal data disclosure notifications	refers to the number of personal data disclosures to law enforcement authorities actually notified to the customer over a predefined period of time (applicable only if the communication of such disclosures is permitted by law).

6.5. Openness, transparency and notice

Description of the context of the requirement

Only if the provider informs the customer about all relevant issues, the cloud service customer is capable of fulfilling its obligation as data controller to assess the lawfulness of the processing of personal data in the cloud. Moreover, the cloud service provider shall make available the information that enable the customer to provide the data subjects with an adequate notice about the processing of their personal data, as required by law.
Notably, transparency in the cloud means it is necessary for the cloud service customer to be made aware of cloud service providers' subcontractors contributing to the provision of the respective cloud service.

Description of the need for SLOs, in addition to information available through certification, adherence to codes of conduct, etc.

Regarding the transfer of customer's personal data to the provider's subcontractors, the WP 29 Opinion highlights the necessity that contracts between the cloud service provider and its subcontractors reflect, in terms of data protection provisions, the stipulations of the contract between cloud service customer and provider.
Furthermore, the cloud service customer consent (which can take the form of a general prior consent) is necessary for subcontracting and the customer may object to changes in the list of the subcontractors. In order to implement these provisions, the list of subcontractors must be made available to the customer.

The processing of certain special categories of data may require compliance with specific regulatory provisions, which may not be covered by standards or certifications schemes of general application. Therefore, it should be specified within the service agreement the possible special categories of data that the service is suitable for.

Description of relevant SLOs

List of tier 1 subcontractors	refers to the cloud service provider's subcontractors involved in the processing of the cloud service customer's personal data.
Special categories of data	refers to the list of the specific categories of personal data (if any), e.g. health-related or financial data or otherwise sensitive data, that the cloud service is suitable for processing, according to applicable standards or regulations.

6.6. Accountability

Description of the context of the requirement

In the field of data protection, accountability often takes a broad meaning and describes the ability of parties to demonstrate that they took appropriate steps to ensure that data protection principles have been implemented.
In this context, IT accountability is particularly important in order to investigate personal data breaches; to this end, the cloud platform should provide reliable monitoring and logging mechanisms, as described in the relevant sections of these Guidelines.
Moreover, cloud service providers should provide documentary evidence of appropriate and effective measures that are designed to deliver the outcomes of the data protection principles (e.g. procedures designed to ensure the identification of all data processing operations, to respond to access requests, designation of data protection officers, etc.). In addition, cloud service customers, as data controllers, should ensure that they are prepared to demonstrate the setting up of the necessary measures to the competent supervisory authority, upon request.

Description of the need for SLOs, in addition to information available through certification, adherence to codes of conduct, etc.

The cloud service provider must notify the could service costumer in the event of a data breach that affects the costumer data. To this end, the cloud service provider shall implement a data breach management policy which will specify the procedures for establishing and communicating data breaches. In this context, the first of the following SLOs implements these principles and allows the customer to evaluate the suitability of the provider's policy.
The second SLO relates to the need to be prepared to demonstrate the setting up of the necessary measures to the competent supervisory authorities, upon request.

Description of relevant SLOs

Personal data breach policy	describes the policy of the cloud service provider regarding data breach .
Documentation	refers to the list of the documents that the provider makes available, in order to demonstrate compliance to data protection requirements and obligations (e.g. procedures to respond to access request, designation of data protection officers, certifications, etc.).

6.7. Geographical location of cloud service customer data

Description of the context of the requirement

Personal data processed in the cloud may be transferred, also by subcontracting, to third countries, whose legislation do not guarantee an adequate level of data protection. This also implies that personal data may be disclosed to foreign law enforcement agency, without a valid EU legal basis.

To minimize these risks, the cloud service customer should verify that the provider guarantees lawfulness of cross-border data transfers, e.g. by framing such transfers with safe harbour arrangements, EC model clauses or binding corporate rules, as appropriate.
To this end, the cloud service customer shall be made aware of the location of data processed in the cloud, as required also by the above-mentioned principles of openness and transparency.

Description of the need for SLOs, in addition to information available through certification, adherence to codes of conduct, etc.

In this context, the following SLOs represent the instruments based on which the cloud service customer is allowed to control the location of its data.

Description of relevant SLOs

Data geolocation list	specifies the geographical location(s) where the cloud service customer data may be stored and processed by the cloud service provider .
Data geolocation selection	specifies whether cloud service customer can choose a given geographical location for the storage of the cloud service customer data.

6.8. Intervenability

Description of the context of the requirement

Directive 95/46/EC gives the data subject the rights of access, rectification, erasure, blocking and objection. Therefore, the cloud service customer must verify that the cloud service provider does not impose technical and organisational obstacles to these requirements, including in cases when data is further processed by subcontractors.

Description of the need for SLOs, in addition to information available through certification, adherence to codes of conduct, etc.

The contract between the cloud service customer and the cloud service provider should stipulate that the provider is obliged to support the customer in facilitating the exercise of data subject rights in a timely and efficient manner[33]. The following SLO aims to define an objective term of reference for these activities.

Description of relevant SLOs

Access request response time	refers to the time period within which the provider shall communicate the information necessary to allow the customer to respond to access requests by the data subjects

[33] See Article 29 WP Opinion, par. 3.4.3.5

Annex – Members of C-SIG on Service Level Agreements[34]

Drafting team	
Van der Wees Arthur	Arthur's Legal
Catteddu Daniele	Cloud Security Alliance
Luna Jesus	Cloud Security Alliance
Edwards Mike	IBM
Schifano Nicolas	Microsoft
Scoca Lucia Maddalena	Telecom Italia
Tagliabue Stefano	Telecom Italia
Participants	
Yeoman Simon	Cloud Industry Forum
Lecina Gerard	Dassault Systemes SA
Adamski Sara	Accenture
Coates Matthew	Accenture
Hampton John	Accenture
Scott Barbakoff	Accenture
Wynne Barbara	Accenture
McDermott Matthew	Access Partnership
Cargill Carl	Adobe
Jolliffe John	Adobe
Oberle Karsten	Alcatel
Ducable Stephane	Amazon
Hayman Chris	Amazon

[34] The Cloud Service Level Agreement Standardisation Guidelines do not necessarily represent the position of any C-SIG SLA subgroup member below.

Pucikova Zuzana	Amazon
Ciavarella Rachele	APCO Worldwide
Lovegrove James	APCO worldwide
Janeczko Jordan	Atos
Juan Ferrer Ana Maria	Atos
Symonds Michael	Atos
Jacobs Danielle	Beltug
Johan Schoofs	Beltug
Schoofs Johan	Beltug
Balogh Rita	BSA
Boué Thomas	BSA
Vindevogel Kevin	Cabinet DN
Rak Massimiliano	CerICT, Italy
De Dobbeleer Elisabeth	CISCO
Gow Christopher	CISCO
Gray Peter	CloudSigma
Hyner Nick	Dell
Parvin Ali	Dell
Riffer Claudia	Deutsche Telekom AG
Dierick Antoon	DLA Piper
O'Conor Mark	DLA Piper
Van Eecke Patrick	DLA Piper
Tabet Said	EMC
Adams Wayne	EMC
Appleton Owen	Emergence Tech
Dekker Marnix	ENISA

Liveri Dimitra	ENISA
Lehtovirta Vesa	Ericsson
Henault Eric	EuroCIO
Becker Bernd	EuroCloud
Czarnowski Aleksander	EuroCloud
Weiss Andreas	EuroCloud
Mingorance Francisco	Europa Insights
Albl Olivier	Fabasoft
Mayrhofer Karl	Fabasoft
Piberhofer Anita	Fabasoft
Woiesinger Bianca	Fabasoft
Ziegler Wolfgang	Fraunhofer
Aubert Antoine	Google
Dickman Peter	Google
Höllwarth Tobias	Höllwarth Consulting
Bednarich Irena	HP
Sage Jonathan	IBM
Spragge Michael	IBM
Butler Joe	Intel
Romao Mario	Intel
White Nick	Intug
Witsenburg Peter	Intug
Zigan Oliver	Itenos
Spindler Caroline	Kdc-Conseil
Rapp Ben	Managed Networks
Kutterer Cornelia	Microsoft

Lange Mark	Microsoft
Windmolders Sigrid	Microsoft
Devaulx Frederic	NIST
Simmon Eric	NIST
Jahan Guillaume	Numergy
Steiner Alexandre	Numergy
Brunet Maël	Open Forum Europa
Cocoru Diana	Open forum Europe
Alhadeff Joseph	Oracle
Hardaway Samantha	Oracle
Thornby Charlotte	Oracle
Nguyen Thanh	Orange
Daloiso Oronzo	Paragon Europe
Hasson Tal	PWC
Kappler Chris	PWC
Finck Stephanie	Salesforce
Giraudon Christine	Salesforce
Mahnke Jürgen	SAP
Dawson Philip	Skyscape Cloud Services
Stewart Nicky	Skyscape Cloud Services
Chantzos Ilias	Symantec
Precsenyi Zoltan	Symantec
Coulaud Mathieu	Syntec Numérique
Christie Jarita	Tech America
Brocca Salvatore Antonio	Telecom Italia
De Belder Margareta	Telecom Italia

Ketmaier Leonardo	Telecom Italia
Sommantico Maximiliano Dario	Telecom Italia
Vela Marimon Cristina	Telefonica
Muscella Silvana	Trust-IT Services Ltd
De la Mar Jurry	T-Systems
Pauly Michael	T-Systems
Neeraj Suri	TU Darmstadt, Germany
Hendrickx Luc	UEAPME