European Commission

# Standards terms and performance criteria in service level agreements for cloud computing services

**FINAL REPORT**

A study prepared for the European Commission
DG Communications Networks, Content & Technology
by:



*Digital Agenda for Europe*

**This study was carried out for the European Commission by**

**time.lex** CVBA - Hans Graux and Jos Dumortier


and

**Spark** Ltd – Patricia Ypma, Jasmine Simpson, Peter McNally, and Marc de Vries


## Internal identification

Contract number: 30-CE-0600116/00-34

# SMART 2013/0039

### DISCLAIMER

By the European Commission, Directorate-General of Communications Networks, Content & Technology.

The information and views set out in this publication are those of the author(s) and do not necessarily reflect the official opinion of the Commission. The Commission does not guarantee the accuracy of the data included in this study. Neither the Commission nor any person acting on the Commission's behalf may be held responsible for the use which may be made of the information contained therein.

ISBN: 978-92-79-50117-3

DOI: 10.2759/07446

## TABLE OF CONTENTS

## EXECUTIVE SUMMARY

This report was prepared by time.lex and Spark in the European Commission's study on "Standards terms and performance criteria in service level agreements for cloud computing services". This Study had two strategic objectives:

- Firstly, it aimed to discover and map any rules with respect to Service Level Agreements (SLAs) in each of the Member States, and to determine the provisions and approaches which are used in practice. To that end the study team has surveyed (a) the terms and metrics used in professional cloud computing service level agreements (CSLAs) and (b) the legal ecosystem surrounding these CSLAs, being the legal framework applying to these contracts in 32 countries (28 EU Member States and 4 EFTA countries).

- Secondly, it aimed to provide suggestions of model SLA provisions that could provide some further stability, certainty and transparency in the cloud market. This was done by drafting (i) a Model SLA text, which can be used as a starting point for the creation of new SLAs or for the assessment of existing ones; and (ii) a checklist for SLAs in general, which can be used as an overview of critical issues that should be clearly addressed by an SLA, without providing model provisions.

Collectively, these two objectives aim to facilitate the use of trustworthy and predictable SLAs in the European cloud market, thus facilitating the adoption of cloud computing in the Digital Single Market.

With respect to the first objective, the present report contains a description of:

- The legislative landscape, describing whether there are specific rules in relation to cloud computing and/or SLAs in the surveyed countries. The report shows that cloud specific/SLA specific legislation is extremely rare, being identified in only two Member States.

- Rules and policies in regulated sectors, describing any specific initiatives (laws, guidelines from regulators, or policies) in the financial, health or public sector that affect the usage of cloud computing and/or SLAs in the surveyed countries. While requirements are virtually never phrased in terms of SLA requirements (i.e. there is no requirement to conclude or rely on SLAs as such), the overviews show that these sectors frequently suggest requirements in relation to security, privacy, availability and continuity, all of which are topics that could be integrated into SLAs.

- SLA terms and models, assessing specifically which types of provisions commonly occur in SLAs in the surveyed countries. The most frequently

recurring provisions relate to availability and support. Metrics to assess compliance with SLA objectives and the remedies available to the customer are however frequently ambiguous or expressed in a non-binding manner; this can jeopardize the value of the SLA to the customer in case of incidents. Extensive carve-outs to responsibility and liability are common.

- Policy and standardisation, indicating whether any global policies or standards are being used to support or promote the use of specific SLAs or standards in the surveyed countries. The study found that while some Member States have developed a fairly advanced policy framework in relationship to cloud computing in general, SLA-specific policies are rare. Regulators and supervisors in specific sectors on the other hand do provide templates and models, as do ICT sector organisations. These mostly are either a skeleton of provisions, or used as guidance with regard to the important concepts / issues to be included in SLAs, often in the form of specific questions and plausible answers.

With respect to the second objective, the present report contains both a Model SLA, and (in Annex I) a checklist that can be used to assess the adequacy of a cloud SLA. The Model SLA was developed by the Study Team on the basis of the collected national inputs, and on the basis of feedback collected through two workshops on 27 November 2014 and on 11 May 2015. The Model SLA was refined on the basis of feedback of the Study Team's Advisory Board, consisting of Profs. Thomas Hoeren, Christian Laux, and Paul Polański.

The Model SLA contains model clauses, but also explanatory comments that clarify which choices were made in the drafting, why these choices were made, and when a user may wish to make other choices. Customization of the Model SLA would always be needed in practice, and to facilitate this process, the checklist in Annex I was produced as a guidance document.

Finally, this report also contains recommendations for the further development and promotion of the Model SLA, via ongoing projects that explore the automated negotiation, comparison and evaluation of SLAs, and also via organizations that aim to provide tools and know-how to cloud providers and cloud users. In this way, the Model SLA can increase awareness in the European Digital Single Market, and act as a useful tool to guide the conclusion and evaluation of SLAs for cloud computing.

# 1. SCOPE AND OBJECTIVES OF THIS REPORT

The European Commission has been active in the area of cloud computing for some time, in close interaction with the cloud industry. In the Commission's Communication on "Unleashing the Potential of Cloud Computing in Europe"[1], it stated its ambition of working towards safe and fair Contract Terms and Conditions for cloud services. This would allow the Commission to propose market oriented measures to support the development of compliant and secure contractual frameworks for cloud computing, attuned to the needs of cloud providers and cloud users across the EU, thus removing or at least reducing uncertainty and stimulating the development and uptake of the European cloud market.

The Communication further stated that the Commission would develop model terms for cloud computing service level agreements for contracts between cloud providers and professional cloud users, taking into account the developing EU acquis in this field.

It stated also that many respondents underline that model Service Level Agreements will help Cloud services to define the rights and responsibilities of all involved parties. User concerns are related among others to data access and portability, change of control and ownership of the data, liability for service failures such as downtime or loss of data, unilateral changes to the contract made by the provider, ownership of data created in cloud applications and dispute resolution.

This document is a report which has been prepared by time.lex and Spark in the European Commission's study on "Standards terms and performance criteria in service level agreements for cloud computing services" (SMART 2013/0039).

An initial objective of this Study was to find out and map the rules with respect to Service Level Agreements (SLAs) in each of the Member States, and to determine the provisions and approaches which are used in practice. A second objective of the Study is to provide suggestions of model SLA provisions that could provide some further stability, certainty and transparency in the cloud market. The findings in relation to both of these objectives are summarized in the present report.

[1] See http://ec.europa.eu/information_society/activities/cloudcomputing/docs/com/com_cloud.pdf

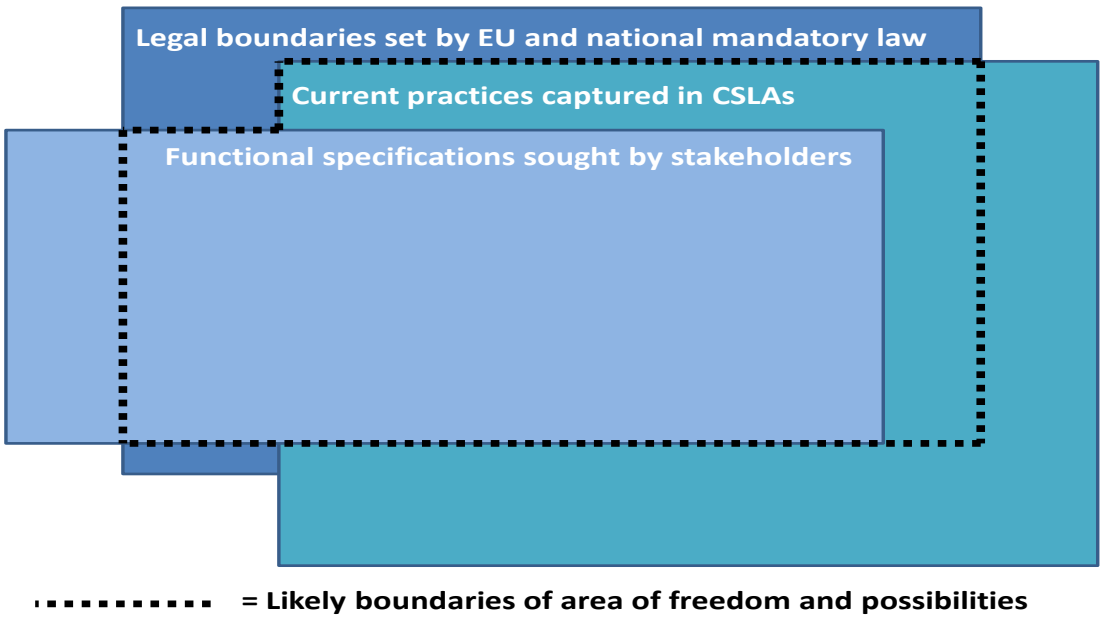
## 2. SURVEY RESULTS

As noted above, a first step in this study consisted of an extensive survey of the relevant legislative and policy framework and Cloud SLA landscape in 32 EU and EFTA Member States. The analysis of this survey was the basis for discussion for this Study's first workshop, and ultimately for the drafting of the Model SLA itself.

The aim of this exercise was to list and cluster the relevant data in order to allow us to see the variety and richness of CSLA contract clauses and metrics, but also to see the common denominators allowing us to identify common ground.

The structure of our analysis is divided into three key subjects that were examined in each national report (legislative landscape, regulated sectors, SLA terms and models, and policy/standardisation).

*Chart 1 – Conceptual model of boundaries and yardsticks for work*




This model was also ultimately the starting point for the Model SLA, created by examining:

- The legal boundaries (corresponding to the sections on legislative landscape and regulated sectors as analysed below);
- Current practices in cloud SLAs (corresponding to the sections on SLA terms/models and policy/standardisation);

- And the functional specifications sought by stakeholders, i.e. the desiderata with respect to cloud SLAs from the perspective of cloud users. These will be based on the recommendations provided in each of the sections below, but also on the basis of the feedback which was collected during the Study's first workshop.

Thus, the intention is to seek out what customers want, and to link this back to current market offerings and legal constraints, in order to provide reasonably justified SLA suggestions.

## 1.1.Legislative landscape

### *1.1.1. General laws and principles*

The first question to be examined in the context of this study is about the existence of specific laws in relation to cloud computing and/or SLAs. This is a crucial step, as such laws will of course need to be taken into account when drafting recommendations, in order to ensure that the study team's proposals are usable across the European Union.

The initial analysis of the feedback from the national experts was instructive, as it confirms the expectation that **cloud specific/SLA specific legislation is extremely rare;** only Slovakia and Luxembourg have specific provisions. In Slovakia Article 2 of its *Coll. on standards for information systems of public administration* contains definitions of cloud computing, cloud service, service level agreement, user, provider, operator and intermediary of cloud services and auditor of cloud. Article 54 (1) ("Standards of provision of cloud computing and use of cloud services") additionally distinguishes and defines IaaS, PaaS, and SaaS as the standard models of provision of cloud services. In Luxemboug, specific provision is made for the recovery of data by the user in the event of the provider's bankruptcy.

Other countries have not yet provided for cloud computing and SLAs in their national legislation, and instead rely on generic contract law. This is beneficial, as it implies that cloud SLAs can be formulated with relative freedom, provided that general provisions of contract law are taken into account.

**General freedom of contracting** between the parties is the standard commonly referenced by the examined countries. When ask about **relevant legislation**, correspondents generally refer to their Civil Codes (15 countries[2]), Commercial Codes (5 countries[3]), and e-commerce/information society services legislation (4 countries[4]). Contractual freedom, as shaped by civil/commercial law (see directly below), is thus the main rule.

[2] Austria, Belgium, Croatia, Greece, Hungary, Italy, Latvia, Lithuania, Malta, the Netherlands, Poland, Portugal, Romania, Slovenia and Spain

[3] Bulgaria, France, Slovakia, Spain, and the United Kingdom

[4] Czech Republic, Latvia, Poland, and Spain

### *1.1.2. Limitations to SLAs*

Given the absence of cloud/SLA specific legislation, national laws are generally not very prescriptive about what types of provisions can be lawfully included in SLAs. Asked about **limitations to the content and scope of SLAs**, the correspondents note that restrictions can notably flow from legislation on general/non-negotiated terms (in 6 countries[5]), legislation on unreasonable/unfair business practices, including obligations to execute in good faith and to abstain from actions which are contrary to good business practices (8 countries[6]); and rules that punish abuse of rights and harm to morality (2 countries[7]).

While the majority of Member States have rules in place designed to protect consumers in B2C contracts, it is interesting to note that some Member States extend the protection to B2B contracts as well, usually where there is unequal bargaining positions such as when one party is an SME[8]. In addition, the obligation to perform contracts up to professional standards is generally well recognised.

### *1.1.3. Notable perspectives on the role of SLAs*

Several respondents note that cloud SLAs are particularly important as a way of specifying more clearly what the **exact obligations of result** under a contract are, noting that, in the absence of SLAs, there is a risk that cloud contracts can be interpreted as professional best efforts contracts without specific obligations of result.

By way of examples on the scope and role of SLAs, the comments provided in relation to Germany, Romania and Switzerland are particularly instructive.

The German response indicates that "SLAs, as part of a basic service contract, should control and ensure the subject matter of the contract which is important under German law, which provides that in absence of an agreement only an 'average performance' can be claimed from the other party. An 'average performance' concerning IT contracts is very difficult to determine." This illustrates the **first role of SLAs: they are a tool that determines the contractual obligations of the service provider.**

[5] France, Germany, Greece, the Netherlands, Portugal, and Spain
[6] Denmark, Finland, Greece, Hungary, Malta, Norway, Sweden, and the United Kingdom
[7] Greece and Poland
[8] France and Netherlands.

The Romanian response provides a more extreme perspective that highlights the importance of SLAs in order to materialise the obligations of a cloud provider: "The SLA of a cloud services contract represents the object of the obligation assumed by the provider, which, according to article. 1226 of the Civil Code, must be determinable. If this condition is not met, the contract is null and void. Therefore, if the contract does not include an SLA (integrated into the contract or attached to the contract) the object of the obligation is not determined or determinable, therefore, the cloud contract is null and void." This perspective illustrates **a second potential role of SLAs, as a manifestation of the obligations under a contract which is crucial to ensure its legal validity**. Under this interpretation, absence of an SLA could result in the nullity of the contract as a whole, unless other clear indications of the contractual obligations of the cloud provider could be identified.

Finally, the Swiss example provides a third important perspective, noting that "SLAs can be looked at in two ways: 1. as a clarification as to what service is actually provided; or 2. SLA as a conditional exclusion of liability. There is no case law clearly determining which of the approaches is relevant under Swiss law, but it can be stated that the first approach seems to be accepted by the legal commentators and the market. Thus, a shortfall to the service that is not so severe to also breach the SLA is not considered a breach of the service agreement." In other words**, a third potential role of SLAs is to act as an indicator of contractual breaches**, thus simplifying discussions on claimed non-compliance.

### *1.1.4. Terms and Conditions*

The correspondents were also requested to comment specifically on the possibility of SLAs being appended to contracts as a part of general terms and conditions, i.e. absent of any negotiations. The consensus perspective was that such **SLAs would be valid and enforceable, conditional on their clear communication to the other party prior to contract conclusion**. In other words, the cloud user needed to be made aware of the existence of the SLAs, and this **awareness must be proven by the cloud provider** in case of disputes.

However, rules on manifestly unreasonably, unfair or imbalanced contracts remain applicable, **and in such cases judges have the right to set SLAs aside, even in B2B contexts**. The respondents note that the distinction between negotiated and non-negotiated contracts will be considered by the judge, but that it is not decisive: even in negotiated contracts, SLAs can still be set aside if their contents are deemed contrary to binding law or manifestly unreasonable, taking into account all relevant circumstances. Several respondents note the severability of unlawful clauses: judges

may set aside only those clauses which are unlawful, leaving into place the remainder of the SLA.

In some countries, there are more stringent rules with regard to liability restrictions, in case a of standard non-negotiable contracts such as in Italy (please see under 2.5 below).

#### *1.1.5. Liability in relation to SLAs*

Cloud contracts and SLAs are not subject to specific liability rules; the same laws and principles apply as for other types of contracts.

Nonetheless, several interesting perspectives and principles can be identified:

- The Swiss correspondent noted that "limitations of warranty need to be contained in the main body of the individual agreement entered into between the customer and the provider in order to be enforceable. They will not be enforceable if they are only mentioned in the terms and conditions and referred to in the individual agreement." This would be an important consideration when drafting model SLAs, as it implies that **liability must be addressed in the main agreement; not in the SLA**.
- Most respondents noted the **impossibility of excluding liability for gross negligence and intentional harm**, even in B2B contexts.
- **Burden of proof for non-compliance should be addressed** as well, as this is an area where national laws can vary as to whether the burden may be shifted to the cloud user.
- **Service credits are not inherently seen as unlawful or damaging, although care should be taken that they are not excessive**, as so-called penalty clauses may be invalidated by courts (e.g. in Bulgaria or Belgium). This principle applies to any **compensatory clause: their lawfulness depends on whether they could have been considered as a reasonable approximation of harm at the outset of the contract**.
- Furthermore, **exclusions of liability may be set aside if they affect an obligation that is "essential" to the service provided**. For instance, the French Supreme Court held that liability limitation clauses are theoretically valid and enforceable, unless they contradict the scope of an essential obligation with regard to the service that has been contracted for by the other party. Hence, limiting one's liability against the breach of an essential obligation is not sufficient, as such, to invalidate the liability limitation clause; it is also necessary to assess, on a case-by-case basis, whether the effect of the

limitation clause is such as to annihilate, in practice, the actual enforceability of an essential obligation. The judge must proceed to an overall appreciation of the economic interests reflected within the contractual agreement in order to assess the proportionality of the liability limitation clause. Similarly, German doctrine holds that parties **cannot exclude liability for defects completely nor can they limit it inequitably** under the terms of the Civil Code. A balanced approach must thus be found.

- In relation to liability, the negotiated nature of the contract can be pertinent as well: Italian law holds that in case of non-negotiable standard terms, exclusion of liability is only valid if the exclusion is accepted (in writing) by the user.

#### *1.1.6. Conclusions and suggestions with regard to model SLA provisions*

The analysis of the general legal landscape would suggest that the following principles need to be taken into account when providing recommendations:

- There are **no specific laws** on cloud contracts and SLAs that restrict the model provisions that can be taken into account;
- SLAs must be **equitable**, or risk being set aside. This principle applies to both B2B and B2C contracts. While the cloud provider is generally the stronger party (and often able to dictate contractual terms), it is not in the provider's interest to apply imbalanced SLAs, as they could be overturned.
- SLAs should be **clear and unambiguous**, given their function of clarifying obligations and specifying when liabilities may be triggered.
- **Liability should generally be addressed in the services agreement, not in the SLA** as such. If service credits are used as a sanctioning mechanism, these may not be so restrictive in scope that violations of the SLA effectively imply no significant negative consequences for the cloud services provider.

### 1.2.Regulated Sectors

As a part of our analysis of the legal landscape, correspondents were requested to specify if they were aware of any rules and/or policies in regulated sectors, and to describe any specific initiatives (laws, guidelines from regulators, or policies). Three sectors were targeted specifically (namely the financial, health and public sector), although correspondents were also asked to provide inputs on any other sectors that they were aware of as being

relevant. The latter question resulted notably in inputs on the gaming sector from Malta.

In the sections below, we will briefly outline the main findings that affect the usage of cloud computing and/or SLAs in the surveyed countries for the examined sectors.

### *3.2.1. Financial sector*

For the financial sector, most countries reported some cloud specific rules, mainly based on the implementation of the MiFiD Directive (Markets in Financial Instruments Directive 2004/39/EC[9]). This Directive defines certain operational requirements with respect to investment firms and regulated markets, which also affect their ability to employ subcontracting or outsourcing services, including for ICT services such as cloud computing:

- 7 countries reported implementations of MiFiD that resulted in non-cloud specific outsourcing guidelines[10];
- 3 countries reported cloud specific ICT outsourcing laws or guidelines (none linked to MiFiD)[11];
- 18 countries reported non-cloud specific ICT outsourcing laws or guidelines which were not linked to MiFiD.[12]

Thus, cloud specific rules are rare, and relate mainly to outsourcing guidelines from national regulators. Where cloud specific rules are available, the Hungarian description provides a good indicator on the types of requirements that can be found: "The Hungarian Financial Supervision Authority issued guidance in 2012 about the risks in cloud computing services at financial institutions. This is aimed at **management, IT and legal faculties of institutions**. Sector-specific laws on outsourcing apply, i.e. sub-processing requires customer approval, the FSA and customer have audit rights,

[9] Directive 2004/39/EC of the European Parliament and of the Council of 21 April 2004 on markets in financial instruments amending Council Directives 85/611/EEC and 93/6/EEC and Directive 2000/12/EC of the European Parliament and of the Council and repealing Council Directive 93/22/EEC

[10] Austria, Cyprus, Denmark, Greece, Ireland, Spain, and the UK

[11] Hungary, Italy, and the Netherlands

[12] Bulgaria, Croatia, Estonia, Finland, France, Iceland, Latvia, Lithuania, Luxembourg, Malta, Norway, Poland, Portugal, Slovakia, Slovenia, Spain, Sweden, and Switzerland

notification of breaches, and other agreement requirements. The outsourcing of critical functions has to allow the financial institution to retain control and supervision."

It is interesting to note that these concerns are not particularly unique to cloud computing. E.g. the Estonian outsourcing guidelines (which are not cloud specific) note that "the following relevant conditions need to be satisfied: **measurement by the customer firm of effective performance of the service provider, supervision and risk management of the outsourced services, measures for performance taken in the event that functions are not provided, and legal, technical, and organisation measures for continuity and regularity, including periodic testing of backup**.

The [Estonian] Financial Supervision Authority issued a guideline for outsourcing in 2006 requiring supervised operators (e.g. investment funds and firms, banks, insurance companies) to regulate outsourcing in their internal and procedural rules. The Estonian Emergency Act 2009 covers **crisis management, including continuous operation of vital services (including banking) in states of emergency including war**. Cloud providers would therefore probably be obligated to ensure the constant application of security measures with regards to the information systems used for the provision of the vital service (banking service) and related information assets. If information systems are located in a foreign country, the provider of the vital service is required to ensure the continuous operation of the service also in a manner and by means not dependent on information systems located in foreign countries. A 2013 decree from the President of the Estonian bank established certain requirements to ensure continuous operation of the core information systems and equipment required for the functioning of a vital service."

**Continuity and availability are thus key concerns**, which are likely to be addressed through SLAs. Thus, practically speaking, **SLAs are an inevitable requirement in the financial services sector**. Other practical requirements relate to accessibility (to enable supervision) and accountability (to enforce existing laws), but these are not cloud specific.

### *3.2.2. Health care*

Health care is of course a heavily regulated sector, given the sensitivity and confidentiality of health related information, which warrant the creation of

stringent requirements. Some European principles recur almost universally in the feedback provided by the correspondents, which also affect the viability of cloud services and SLAs.

Firstly, **data protection** is a near-universally quoted concern. The Data Protection Directive 95/46/EC considers the processing of health related information to be particularly sensitive, and requires Member States to impose specific requirements (including in relation to security and confidentiality) before health information may be processed. These requirements of course apply to cloud computing as well. Most countries do not flag any cloud specific data protection requirements or guidelines, but there are some exceptions.

In **Croatia**, the Regulation on the Procedure for Storage and Special Measures relating to the Technical Protection of Special Categories of Personal Data lays down detailed requirements on how certain categories of data are dealt with, relying on **ISO standards 27001 and 17799 (27002)**. In **Hungary**, the National Authority for Data Protection and Freedom of Information **opposes the processing of health related information in the cloud altogether**; however, this is a recommendation, and cloud usage for health information is not altogether prohibited if the relevant laws are complied with. The **Slovenian** DPA has similarly provided **guidelines on eHealth outsourcing**, which would also apply to the cloud.

Apart from data protection, **rules on patient rights, confidentiality and professional ethics** can also impact the permissibility of cloud computing. Most of these are relatively high level, and do not contain cloud/SLA specific guidance or requirements. Technical issues are however occasionally broached, as in the Portuguese Code of Medical Ethics, which requires the use of support systems, quality control and evaluation methodologies. Telemedicine systems should **encrypt** data, including names.

Finally, a number of countries have implemented **general eHealth legislation and policies**, which have an impact on how cloud computing can be used. These include the following examples:

- The **Austrian** Act on Health Telematics 2012 § 6 states that health data stored in the cloud must be **encrypted**.
- **Belgium** has established an eHealth platform (created by the Law of 21/8/2008 as a federal public body which sets rules and technical specifications for e-health in Belgium), including stringent requirements that any software (including cloud services) must meet. This includes a **registration requirement**

**with the eHealth platform**. Technical rules govern security, privacy and other requirements.

- The **Estonian** Health Services Organisation Act 2001 regulates the maintenance of health records, and stipulates that **use of the standards of the Health Information System is mandatory e.g. integrity and authenticity of records**.
- In France, only providers **accredited by the Ministry of Health** may host patient data. Accreditation is meant to ensure that these actors will engage in the storage and preservation of health data in accordance with the procedures defined by law (Art L1111-8 of the Public Health Code (*Code de la santé publique)*. In order to obtain accreditation, private actors must ensure **confidentiality, traceability, consent, and security**.
- In the **Netherlands**, an **eHealth specific standard** has been developed (NEN 7510) by the Dutch standardisation institute, which is **based on ISO 27799, ISO/IEC 27002 and ISO/IEC 27001**.
- The **Polish** Law on Healthcare Information Systems which entered into force in 2012 established rules for the operation of such systems in Poland. The healthcare information system is based on distributed databases, which are being operated by service providers, payers, the Ministry of Health and other subjects obliged to process data concerning healthcare services.
- Finally, in the **United Kingdom**, planning and procurement guides are published by NHS England. There are guidelines for the health industry on 'what to look for' within CSLAs given the risks associated with cloud computing services for healthcare providers. The Health and Social Care Information Centre has an NHS Information Governance Toolkit[13] that measures services against the legal and regulatory requirements (as prescribed by the DoH for NHS England) of contracting with third parties. Requirements include references to **relevant standards (again, notably ISO/IEC 27002 and ISO/IEC 27001**). Contracts should include, inter alia, **penalties for breach**, with most of the other provisions related to data protection. In addition, adoption of new processes, services, systems and other information assets should be implemented in a way that "does not result in an adverse impact on information quality or a breach of information security, confidentiality or data protection requirements" (Req. No 11/210). This includes having adequate security "to ensure that personal information is protected from unlawful or unauthorised

[13] See https://www.igt.hscic.gov.uk/

access and from accidental loss, destruction or damage". There are guidelines that identify the requirement to manage risk to data and systems that extend to cloud systems, but the specific requirements are predominantly managed locally and vary in implementation.

It is worth noting that eHealth is thus relatively strictly regulated, with references to security standards such as the ISO 27001 series being fairly commonplace. While **no country forbids cloud computing in health care as such**, data protection is seen as a sufficiently serious concern that at least one DPA (in Hungary) counsels against it, and at least two others (Belgium and France) have implemented requirements that certain cloud based solutions must be **notified to public administrations in advance**.

### *3.2.3. Public sector*

The public sector similarly has its reasons for implementing specific rules and policies in relation to cloud computing. This is mainly because of the wide scope of its data collection (spanning potentially all citizens and businesses within its borders), and because of the sensitivity of some data sets (e.g. tax related information). Furthermore, data security and control are crucial challenges, given the need for continuity of government services. For these reasons, it could be anticipated that cloud/SLA specific requirements may be in place.

Based on the responses of the correspondents, a few key trends can be identified.

- Principally, there is **virtually no cloud specific legislation** in the surveyed countries, with the sole two exceptions being the Slovakian Decree No. 55/2014 Coll. on standards for information systems of public administration, and the Italian Code of Digital Public Administration. Strictly speaking, both of these are eGovernment laws (of which there are a few, as noted below), but they stand out as the only legislation which explicitly mentions cloud computing concepts (such as SaaS, cloud computing itself, cloud service, service level agreement, user, provider, operator and intermediary of cloud services and auditor of cloud).
- There are however **a multitude of eGovernment laws which would also apply to cloud services**; such laws have been

identified in 13 countries[14]. The Lithuanian example is instructive on typical requirements, noting that "a written outsourcing agreement must contain provisions on additional services, security and confidentiality, liability, communication, audit and control, etc. More detailed requirements, which also affect outsourcing, are provided in the Description of General Electronic Information Security Requirements which cover identification, authorization, physical access, back-up, confidentiality, encryption, etc. and include minimum levels of availability, 70-99% yearly". Sweden's *Kammarkollegiet*, the public agency procuring services for public authorities in Sweden, has issued SLAs that are a part of the framework agreements for online or cloud services[15]. While this is not an established custom yet, both the SLAs are part of the framework for cloud services offered to public authorities with regards to office support and services supporting e-government.

- Finally, 11 countries[16] have implemented **cloud policies that specify how and to what extent cloud services may be used**. An interesting example is the UK, where the G-Cloud was launched in 2012, as an IaaS and PaaS platform. This is to facilitate the procurement of cloud services through frameworks and the CloudStore. Approved providers for cloud services in the public sector can therefore be easily identified. Data is categorised under "Business Impact Levels" depending on the security required. Services accredited to BIL2 (e.g. Windows Azure, Office 365) can be used by the majority of the public sector, whereas BIL3 comprises restricted data and is limited to certain private cloud services. As the impact level of data and systems increases, the cost typically increases significantly, as does the unique nature of the service. The Cabinet Office has published guides for public sector institutions using the CloudStore. There is a trend to favour or require internal clouds only; such policies have been identified in Bulgaria, France, Greece, Latvia, and Romania.

[14] Bulgaria, the Czech Republic, Estonia, Finland, Germany, Greece, Lithuania, Norway, Portugal, Romania, Slovenia, Spain, and Sweden

[15] See https://www.avropa.se/PageFiles/21659/Bilaga%20A9%20SLA.pdf

[16] Austria, Bulgaria, Estonia, Finland, France, Greece, Hungary, the Netherlands, Romania, Sweden, and the UK.

Generally, cloud specific rules are limited, but ICT procurement laws and policies can sometimes shed some light on appropriate practices in each Member State.

### *3.2.4. Gaming*

Finally, as noted earlier, the Maltese correspondent noted specific rules for online gaming. The Remote Gaming Regulations (Subsidiary Legislation 438.04) require a licence for the operation, selling or promotion of remote gaming in or from Malta. The Regulations are technology-neutral in principle, but additional guidance in the form of standard emanating from the Lotteries and Gaming Authority has been called for so as to ensure the benefits of cloud computing can be utilized whilst minimising risk.

In 2013 the Lotteries and Gaming Authority started a feasibility assessment regarding cloud computing in gaming (not yet published). In October 2013, an MoU was signed between Malta and Alderney (part of the Channel Islands) to set up 'business-friendly' environments for e-gaming. Cloud computing is one area in which there will be cooperation to improve the standard of regulation.

In addition to gaming in the gambling sense, there have been recent moves to support a 'Digital Gaming Strategy' in Malta focused on video games, with a report of 2012 specifying that many providers are moving to cloud computing specifically to find web gaming solutions.

### *3.2.5. Conclusions and suggestions with regard to model SLA provisions*

Most of the regulated sectors are subject to ICT procurement and usage rules, but cloud or SLA specific rules are altogether fairly rare. Where they can in fact be found, the following elements can be highlighted:

- Generally, **health care appears to be the most strictly regulated sector,** with strong requirements in terms of security, confidentiality and privacy;
- **Security requirements generally reference international standards, particularly the ISO 27000 family.** It is thus advisable to align any SLA recommendations with such international standards;

- **Sector specific norms generally emanate from specialised supervisors and regulators, not from legislation.** This suggests that recommendations are appropriate, but legislative intervention is not.
- **Key topics addressed by SLA recommendations relate to availability/uptime, continuity, support, and security.**
- **Especially in the financial and health care sectors, external supervision/auditing are commonly called upon to ensure compliance.** In the public sector this requirement is less common, likely because of the greater use of private clouds where external supervision would be unnecessary.

## 1.3.SLA terms and models

### *1.3.1. Service Level Agreements*

The assessment of SLA terms in use in Member States was **limited by the lack of availability of SLAs of many national providers**. The level of availability tends to vary between Member States. The observations made in relation to the SLA offering of national providers in many Member States are thus based on samples of SLA terms which are available.

Some national providers publish their SLA terms online, while others do not. **National providers who do publish the SLA terms do so with varying degrees of precision/elaboration**: some merely mention a guarantee to provide a certain level of service in the FAQ section of the website, others mention levels of service as part of the terms of service generally, while others publish SLAs in the true sense. Non-publication of SLA terms by national providers may result from the fact that they offer bespoke SLAs, or particularly in the case of smaller providers the desire to avoid the extra cost of drafting and maintaining SLAs. It is difficult to categorise the Member States by level of detail provided by national providers; often SLAs with varying degrees of detail are evident in a single Member State (for example HR, IE and CH all have national providers offering percentages of availability, in addition to providers who make non-measurable statements regarding availability).

SLAs for global providers (such as Google and Microsoft) on the other hand, are generally available online, tend to provide detailed metrics and tend to show little or no variation by jurisdiction (the main variation being adaptation to the language of the jurisdiction). **Global providers have a presence in all countries examined.** As to the format, the SLA terms are often set out in a separate document, which is referred to by the terms of service, or accessible by a hyperlink and linked to the cloud contract as an attachment.

Standard SLAs in IS are a specific case, due to a culture of deferring to general legal principles, which are not spelled out in contracts, but which are widely known and accepted. Bespoke contracts are usually more detailed/longer. However, many of the more bespoke cloud computing services providers are SMEs with limited funds and manpower affecting their ability prepare contractual documentation that adequately meets their needs and protects their basic interests in this respect.

### *1.3.2. Negotiability*

SLAs of global providers tend to be standard and non-negotiable. While national providers often provide standard non-negotiable SLAs, there is generally more of a tendency among smaller national providers to provide bespoke cloud solutions, where the SLA is more likely to be negotiated.

### *1.3.3. Service Availability*

It is rare for an SLA not to provide for availability in some way. The examined **SLAs provide for availability in one of 3 ways**:

i. Availability expressed as a percentage of uptime, accompanied by a detailed formula, while what is included or excluded from the calculation of uptime is specified (usually the case for global providers or national providers in some Member States, such as in Bulgaria, Estonia, Sweden);
ii. Availability expressed as a percentage of uptime, with no detailed formulae as to how uptime is to be calculated (e.g. national providers in Ireland, Croatia, Lithuania, Romania); or
iii. General statements providing a non-measurable commitment as to availability (evident in Switzerland, Croatia, Ireland, Liechtenstein).

The SLAs of global providers generally guarantee service availability as a **percentage of "uptime", while specifying what is included or excluded from the calculation of uptime.** For example, the SLA may guarantee 99.9% uptime, while service interruptions of up to 10 minutes and scheduled maintenance do not count as downtime. Alternatively, another provider may assert a lower headline availability figure of 99.5% but count unscheduled service interruptions in excess of 5 minutes as downtime. It is not always easy to identify which availability level is better for the user. Usually availability is calculated on a monthly basis. In addition, it is not uncommon for global providers to offer different levels of availability for different products.

The examined SLAs of national providers varied in terms of detail. In some Member States, it was noted that the national providers take their lead from the global providers present on the market, and their SLAs are drafted to reflect this. For example, an SLA of one national provider which was examined in Estonia guarantees 100% uptime, while 15 consecutive minutes of downtime is required to claim compensation. In other cases, the SLAs contain **promises such as the provision of 99% uptime, but do not provide detailed formulae as to the calculation of uptime.** Others make **general statements providing a non-measurable commitment**, such as "best efforts to provide high service availability" (noted in Croatia), or stating "we strive to keeping our services available 24 hours 7 days a week (but do not guarantee)" (noted in Switzerland).

### *1.3.4. Remedies*

For standard SLAs, where a measureable availability commitment is provided, it is usually accompanied by remedies. This was noted in respect of national and global providers. In some Member States such as Switzerland, a lack of express provisions regarding remedies was noted. However, this seems to be related to the lack of a measurable commitment regarding availability, and generally **instances where SLAs do not provide a measurable availability commitment (Slovenia, Spain, Iceland, Denmark) do not seem to be accompanied by commitments as to remedies.** In Malta, a lack of detail was noted in the SLAs of smaller national providers relating to the manner in which service credits are to be claimed.

**Remedies usually take the form of service credits.** The service credits are usually expressed as a percentage of the monthly fee, and subject to an overall cap (anything between 30%-100% of the monthly service charge). The service credits often operate on a sliding scale (10%, 25%, 50% was noted in the Netherlands) depending on the extent to which availability falls short of the guaranteed percentage.

**In relation to bespoke SLAs, there is some evidence of alternative remedies being provided for.** For example, in the Netherlands, one system currently in use consists of using yellow and red cards, similar to those in football games: when a service has – during a month (or another agreed measure period) - not reached the agreed level of service, the provider receives a yellow card; when this happens again a red card is issued. The penalty effect of the cards can be nullified through an 'earn back' scheme; by offering a better service in the following measured period or by offering added services, such as free IT consultancy (which may have added value for the cloud provider too). The effect of negotiability of the SLA on the remedies was echoed in relation to Germany.

Many providers impose **time limits for claiming remedies**, i.e. customers must notify the provider within 14 days in EE, 30 days under the Google T&Cs. In some instances, the provider will insert a term stating that any **remedy will be at the discretion of the provider** (noted in the context of an Irish national provider's SLA).

### *1.3.5. Exclusion of liability*

Many SLAs seek to limit liability but providers may be prevented from doing so by legislation. SLAs often **exclude liability for ordinary negligence**, e.g. Croatia, Liechtenstein, though **not for gross negligence, or mal-intent**, e.g. Austria, Bulgaria. A leading Belgian providers accepts liability only for deception or serious misconduct. The Swedish Standard Contracts SLA excludes liability for all damages except caused by the providers gross negligence or deliberate malice, and in Switzerland it is common to exclude liability for any act or omission which is not intentional or grossly negligent. **Force majeure events** are routinely covered by an exclusion of liability, e.g. Belgium, Bulgaria, Croatia, Denmark, Ireland, Latvia, Malta, Netherlands, Poland, Portugal, UK. Liability may be excluded for unavailability due to **scheduled maintenance**, e.g. Estonia, Latvia, UK, or **customer's activity or equipment** e.g. Belgium, Croatia, Latvia, Poland, Portugal, Romania, UK. Liability for **failures due to third parties** may be excluded e.g. Finland, Malta, Poland, Portugal, UK, or **anything outside the providers reasonable control**, e.g. Poland. Liability for **interruptions or disruptions** are excluded by providers in Denmark, Norway, **service outages and performance issues** in Estonia, Norway, UK. Liability for **indirect or consequential loss** may be expressly excluded e.g. in Austria, Belgium, Hungary. Global providers exclude liability for **loss of data** and national providers have often followed suit and omitted any obligations in this area (e.g. Belgium, Norway). Norwegian providers include exclusions of liability for **breach of confidentiality and non-compliance with regulatory requirements**.

### *1.3.6. Data migration*

**Data migration is not usually included** in SLAs, and providers are rarely obliged to ensure portability. A lawsuit in Austria has confirmed that providers do not have to provide the data in a format requested by the customer. However bespoke agreements may cover this area, and outsourcing agreements in the UK would usually include such provisions. The Swedish Standard Contracts SLA requires customer data, and, where applicable, software, to be returned on termination of the contract. In addition, the supplier must assist the customer to a reasonable extent in transferring data, and may charge for this. For services to the public sector in Spain, providers should guarantee portability under the National Interoperability Framework. **Some**

**SLAs included provisions on timing** (in SK: the user should migrate data within 10 days, provider should return data within 5 days), **medium** (in Slovakia: CD or as otherwise agreed, in standard structure format, in Finland the file format is also specified in some SLAs) and **responsibility for migration** (user moves data at own risk).

Providers may be required to destroy the data at the termination of agreement, e.g. as required in Latvia by the Data State Inspectorate Recommendation on Security of Personal Data Processing 2013, or to store it for a reasonable period of time (e.g. Romania). Migration may be included elsewhere in the contract (Portugal) and in relation to the provider: in Ireland, the Data Protection Commissioner requires that the cloud provider must have a written agreement with any entity processing data on its behalf, which sets out the right of the cloud provider either to remove data from the processor, or transfer it to another provider. Reverse engineering rules which oblige computer programme interoperability could also arguably apply to software (Portugal). The ITIL (IT services management framework) influences providers in when drafting data migration provisions in Norway. Migration could be covered by the new supplier; such as in France, where a provider may facilitate customers who wish to move to their services, even where the incumbent provider has no such platform. Portability may also be covered in outsourcing agreements (UK, Czech Republic).

### *1.3.7. Models*

**Most Member States do not have standard models** for the formation of SLAs, however there is some guidance published at national level. In Austria, 2012 **recommendations were published for providers setting up terms and conditions**, by the Chamber of Commerce, Austrian Standards, EuroCloud Austria, the Association of Data Processing (ADV), and IT cluster Vienna. These suggest including "sufficiently detailed provisions" on, inter alia, data backup and return on termination, customer support and response times, error or fault management procedures, compliance with SLAs, and monitoring and reporting of availability levels.

While there are no model contracts in Germany, the Institute for Standardisation (DIN) develops SLA practices for different industries, and the DIN SPEC 1041 (05/2010) determines that a SLA is a "contractual term about quality and quantity of a service performance which looks at provable criteria". The Federal Office for Information Security develops security settings for Cloud Service Providers and informs users about security aspects in CSLAs. The Protection Level Agreements study contains standardised guidelines for SLAs for contracts concerning IT projects between public bodies and providers in order to ensure a higher security level. The government has commissioned experts to provide recommendations for users and providers, such as

the Commissioner of the Federal Government for Communication Technology and Trusted Cloud. These are however voluntary and provide no models.
In Norway, the Agency for Public Management and eGovernment (Difi) has published several standard contracts, but these are not applicable to cloud services, and **standard terms have been criticised for favouring either the user or the provider**, depending on which interest group has designed it. In Romania the Eurocloud Cloud Computing Catalogue may be used when writing and negotiating contracts and SLAs, as well as several internet templates.

Sweden has the most advanced model in use, developed by The Swedish IT and Telecom Industries organization: the Cloud Computing Standard Contract, published in October 2010. This covers general terms & conditions, special conditions for SaaS, and SLAs. The model has been criticized however for being too provider-friendly (e.g. by capping liability and limiting damages). It is also optional; parties must specify and regulate service levels themselves. The standard SLA is also quite narrow in scope, only covering availability of the service and customer support. The parties must thus agree separately on remedies; if no such price reduction is agreed the customer only has the right to a reasonable reduction of the fees.

### *1.3.8. Conclusions and suggestions with regard to Model SLA*

- In SLAs, often the headline figures regarding availability guarantee and remedies are clear. However, sometimes the manner of calculating uptime, and how issues such as how scheduled maintenance as categorised, along with terms affecting how service credits can be claimed may render the seemingly generous guarantee ineffective. Rather than a model term focusing on the percentage availability or scale of the service credits, it might be **more beneficial to users to have model terms defining issues such as uptime and downtime.**
- When availability is expressed in a non-measurable way, remedies are also generally not specified, meaning that **in some cases unsatisfied users must look to the general contract or tort law of the Member State for remedies.** In these situations, both users and providers could benefit from the clarity (and potential reduction in litigation costs) which model terms could bring.
- **Exclusion of liability is common**, with providers generally excluding liability for **ordinary negligence but not for gross negligence** or intentional harm. Specific exclusions are also common (e.g. force majeure, failure due to third party etc).
- **Approaches to data migration lack consistency**, and are usually seen as an **"extra" rather than key area** of SLAs.
- **Standard models are rare and are not widely used**. They are not always perceived as being balanced. For further details, please see section 5 on policy and standardisation.

## 1.4.Policy and standardisation

### *1.4.1. National Cloud policy developments*

Generally, there is not yet a prevalence of a detailed and coherent policy relating to cloud computing, **or SLAs in particular**. In most countries (28), there is a general cloud strategy, which is addressed at the public sector and intended to stimulate the update of cloud computing services and stipulates the important legal and security issues surrounding the acquisition of cloud computing services (Austria, Czech Republic, France, Denmark, Finland Germany, Hungary, Iceland, Ireland, Italy, Lithuania, Malta, Netherlands, Poland, Slovakia, Slovenia, Spain). No Policy (developments) were noted in Liechtenstein and Portugal[17].

Some notable developments, where policy guidelines were **issued to the public sector** with regard to the use of cloud computing services, are the following:

- The Nordic Council of Ministers'[18] informal forum for IT directors in December 2013 issued a "Legal guide to public organisation cloud sourcing in the Nordic countries." The aim of the guide is "to provide a practical tool for public organization buyers in the Nordic countries to ensure legal compliance, contractual efficiency and proper handling of risks and selection of safety measures in situations where the organisation is contemplating to cloud-source certain IT services."
- In Germany the BMWi has launched two national research projects to investigate cloud based services in the public sector, within the so-called "Trusted Cloud" project.
- In the UK, G-Cloud provides a database for procurement of cloud services in the public sector and there is a Cabinet Office guide for this tool.

Thus, several policy documents indicate the manner in which the public sector will take up the cloud, i.e. whether they will use a public or community cloud. If these

[17] However, the acquisition of Cloud Computing by the Public sector is regulated as an acquisition of services by the Code of Public Contracts 2008, which is complemented by the Open Standards Act 2011, which mandates public bodies to contract computer software based upon open standards concerning digital information processing in the Public Administration with a view to promoting technological freedom of citizens and organizations and the interoperability of computer systems in the state.

[18] Denmark, Finland, Iceland, Norway, Sweden and the Faroe Islands, Greenland and Åland work together in the official Nordic co-operation.

documents are followed by public sector users, it could have the effect of limiting the types of cloud options of which they can avail.

A common governmental (community) cloud is envisaged in Bulgaria, France (the first government administration cloud service in France was adopted: a private cloud solution developed by Accenture), Latvia (establishment of a Public Sector Cloud Computing Centre, which would be the responsible institution for supplying Latvia's public sector with the necessary and common cloud computing services), The Netherlands ('Rijkscloud') and Slovakia (the creation of two centralized data centres for the government).

### *1.4.2. Protection of SMEs*

With regard to the protection of SMEs, it is worth mentioning that in most Member States, SMEs are not protected in the same way as consumers, despite their relative low bargaining power in contracting. In Croatia the Ministry of Entrepreneurship and Crafts offers advice for SMEs in its e-business publications (supported by EU funds), which also include sections with advice specifically devoted to **the issue of SME uptake of cloud computing services**. These sections largely focus on benefits of the uptake of cloud computing and there is specific advice for SMEs with examples of services. **However, no guidance on service level (agreements) is included.**

### *1.4.3. Development of (voluntary) standards*

*Adherence to international standards*

In most Member States, the international ISO 27000 series of standards are adhered with regards to SLAs (while adherence to international standards was not noted in Croatia, Denmark, Finland, Latvia, Liechtenstein, Portugal, Switzerland). It was noted that in the Czech Republic, some national standard legal requirements are based on the structure and terms of the ISO 27k and it is predicted that both industry and the public sector will stick to it. The International standard ITIL is relied on in both Germany – where standard supervision is mainly guaranteed by certification of ITIL - and Norway, where the ITIL framework is popular in relation to migration/transition. Cloud Security Alliance's[19] 'Cloud Controls' was also mentioned, with regard to the

[19] The Cloud Security Alliance (CSA) is a not-for-profit organization with a mission to promote the use of best practices for providing security assurance within Cloud Computing, and to provide education on the uses of Cloud Computing to help secure all other forms of computing. The

provision of fundamental security principles, to guide cloud vendors and to assist prospective cloud customers in assessing the overall security risk of a cloud provider (e.g. Hungary). Other international standards mentioned were SAS70 (Austria, France, Poland), COBIT, SSAE16/ESAE3402, EuroCloud Star Audit, FedRamp, CSA, PCI DSS (Austria).

*Development of national standards*

In relation to national standards, most Member States have not had much detailed development in this area, especially when it concerns service levels. In 16 countries (Austria, Bulgaria, Czech Republic, Finland, France, Germany, Denmark, Ireland, Netherlands, Romania, Spain, Slovakia[20], Slovenia, Romania, Switzerland and the UK), work is being done on the development of a national standard for cloud computing services, initiated by either national standard setting bodies, Eurocloud divisions, users associations and / or industry. The majority of these standards do not contain specific guidance or standards on service levels, but rather focus on security standards. As expected, adherence is (currently) mostly on a voluntary basis. Notable developments with regard to national standards are:

a.) Initiatives from national standardisation bodies:

- National Standards Authority of Ireland (NSAI), through its ICT Standards Consultative Committee (ICTSCC), maintains active engagement across all relevant Cloud domains covering Cloud Computing, SOA, IT Security and IT Governance via relevant Irish mirror committees of the international JTC 1 system.

- The NSAI has published **SwiFT 10:2012**, a document intended for use by businesses of all sizes considering the adoption of cloud computing. It sets out a generic series of questions which businesses should take into account when engaging a cloud provider. **A number of the questions relate to CSLAs**, where especially questions on 'Service Availability' are relevant, for example:

    - What are customer uptime expectations?
    - What are the financial and/or liability management implications of a service outage?
    - Are service credits expressed on a sole remedy or sole liability basis or other form of reference to the contract liability exclusion or limitation provisions?
    - Are the consequences of such references understood?

Cloud Security Alliance is led by a broad coalition of industry practitioners, corporations, associations and other key stakeholders.

[20] Mainly through legislation.

While this may result in awareness among cloud customers of the right questions to ask in relation to CSLAs, **it does not have the effect of setting a standard in terms of the CSLAs themselves**.

- The German Institute for Standardisation has established **DIN SPEC 1041 (05/2010)** which determines that a SLA is a "contractual term about quality and quantity of a service performance which looks at provable criteria".

- The Spanish Association for Standardisation and Certification, AENOR, is contributing to Distributed Application Platforms and Services (DAPS), with a working group and a study group devoted to Cloud Computing in the Joint Technical Committee ISO/IEC JTC 1/SC 38. The norm, still being drafted, is called PNE 71380 **Information Technology, Cloud Computing, Vocabulary and definition**s.

- The British Standards Institution, the UK standards body, has partnered with the Cloud Security Alliance, an international organisation, to produce the **CSA STAR certification**, an enhancement to the ISO/IEC 27001 information **security standard** that addresses specific **security issues related to cloud computing**. In addition, the Cloud Industry Forum (a provider industry body) has issued a **Code of Guidance** intended to improve transparency. Providers can **self-certify or be audited** for adherence to this Code.

b.) Industry initiatives

- In the Czech Republic an Industry initiative has offered **a voluntary standard for cloud services** to the public sector. This initiative aims at the establishment of a common understanding of **standard security requirements** for the use of cloud services.

- The Danish Association of IT hosting Companies (BFIH) in 2011 introduced a quality mark called "**Hostingmærket**" ("The Hosting Mark") which requires BFIH's members to d**raft their SLAs in a transparent manner**, e.g. describing the performance in graphs and tables, which follow a common BFIH definition. The service providers may decide on the specific SLAs themselves, as long as they follow the BFIH definitions. Moreover, the customers must at all times have access to the applicable SLA.

- In Finland, the Central Chamber of Commerce, the Finnish Software Entrepreneurs Association, the Finnish Association of Purchasing and Logistics (LOGY), the Federation of Finnish Technology Industries and the Finnish Information

Processing Association jointly drafted the **IT2010 general terms and conditions**. These are widely known and used in whole or in part throughout the IT sector. However, **terms relevant to the cloud computing sector are not commonly used** as many companies prefer to draft their own terms. These terms include, among other things, conditions for **data security, backups and the processing of personal data, as well as limitation of liabilities**.

- In the Netherlands, the open standard "**CloudControls**" is being developed by the industry (CloudVPS and KPMG as co-developers). This consists of a set of measures aimed to control 61 identified risks (outsourcing, multi-tenancy). In addition, the Dutch standards-setting body NEN aims to develop The Dutch Practice Guidelines 5317, which will consist of practice guidelines on cloud computing in the form of **open standards for cloud computing, covering a number of areas including SLAs.**

- The Swedish IT and Telecom Industries' Cloud Computing has developed a **Standard Contract**, which includes: a.) General Terms & Conditions (applicable for all types of cloud services); b.)Special Conditions Supplier's Cloud Computing Application (applicable for SaaS); c.) Service Levels for Cloud Computing (SLA).

c.) <u>Other codes / guidelines</u>

- In Austria, recommendations were published in 2012 for providers setting up terms and conditions, by the Chamber of Commerce, Austrian Standards, EuroCloud Austria, the Association of Data Processing (ADV), and IT cluster Vienna. It consists of a 'catalogue of recommended contractual elements that should be incorporated into the General Terms and Conditions and Service Level Agreement' for cloud service providers. The list does not contain suggested legal wording for provisions as 'the specific wordings may vary substantially according to the respective cloud service context'. The catalogue includes relevant topics with regard to SLAs, where certain items are suggested to be taken into account and described in sufficient detail, such as:

    - **2.2 Rules concerning the content of the services**: '*sufficiently detailed description of the cloud service itself and the nature of the cloud service, e.g., Infrastructure as a Service (IaaS), etc*.'
    - **2.3 Rules concerning the implementation of the services:** '*sufficiently detailed description trial versions of the service*', *possibilities for customising* and *associated costs, training,* etc.
    - **2.4 Rules concerning operations of the services:** *'sufficiently detailed description Representation of release management process', 'error or fault management processes',* etc.

- **2.5 Rules concerning the availability of the cloud service: '***Detailed regulations for communication channels for support*', '*the use of a supporting system, such as a ticketing system'.*

The rules given thus do not give much details on the actual service levels, but can be seen as guidance with regard to issues to take into account when negotiating an SLA.

- The German Federal Office for Information Security (Bundesamt für Sicherheit in der Informatonstechnik, BSI) develops **security settings for Cloud Service Providers** and informs users about security aspects in CSLAs. Moreover the BSI is conducting research on how SLAs for IT contracts could help to observe security arrangements, especially in public administration (Protection Level Agreements, PLA study). The PLA study of the BSI contains **standardised guidelines and elements of SLAs**, which will be used in contracts concerning IT projects between public bodies and providers in order to ensure a **higher security level**. In addition, the working group "legal framework" within the "Trusted Cloud" project has developed a **guideline for contracting for cloud services which gives advice on SLAs**. Additionally the Federal Ministry for Economic Affairs and Energy has published a study about standardising in the area of Cloud Computing based on the results of the "Trusted Cloud" programme, which deals with **the possibilities of SLAs in standardising and quality management**.

- In Greece there has been some movement to introduce **standards for data portability and migration**, namely the Operation Programme Digital Convergence guidelines on procurement of cloud services, and 2008/10/11 laws on eGovernment, open standards and interoperability. In Ireland a Cloud Service **Trust Label is being developed** by the Irish Centre for Cloud Computing and Commerce, to monitor SLA performance.

- The Irish Centre for Cloud Computing and Commerce is seeking to develop a Cloud Service Trust Label to monitor SLA performance.

- In Romania "**the Cloud Computing Catalogue**" - a publication to which representatives of cloud providers and of the Romanian division of Eurocloud have contributed - provides a series of recommendations with regard to issues which are important to be regulated by the cloud contract, with the aim of **setting standards of good practice in cloud contracts**.

- Kammarkollegiet, the public agency procuring services for public authorities in Sweden, has issued SLAs that are a part of the framework agreements for online or cloud services. As far as we know, these are not publically available.

- In Switzerland, the **government recently assessed a number of standards** in the field of cloud computing and favoured the certification promoted by the **EuroCloud** network.

It seems that national standard setting bodies and national divisions of Eurocloud play an important role as facilitators of the development of voluntary standard setting frameworks by various stakeholders, by bringing them together, helping them to identify best practices and making international, European and national codes of practice available.

## 1.5.Conclusions and suggestions with regard to Model SLA

While in some countries (the UK, Germany, Ireland) the policy framework is more advanced than in others, there is generally not yet a prevalence of a detailed and coherent policy relating to cloud computing, **or SLAs in particular**. However, it is expected that this will evolve in parallel with the uptake of cloud computing services in the coming years. The same applies to the development of standards, where initiatives are being taken by the public sector, standardising bodies and industry. There are no standard as we typically understand the term in the IT sector, however standardisation bodies, sometimes in cooperation with governmental organisations public and industry, have publications / initiatives in the area that can be taken as guidance. Emerging national standards are mostly focussed on security issues (sometimes referring to international ISO standards such as the 27000 series) and are based on voluntary adherence. Examples, where standards relevant to service levels seem to be developed further, are **Austria, Denmark, Ireland and Germany**. These mostly are either a skeleton of provisions that can be further completed by the parties when negotiating the SLA, or used as a guidance with regard to the important concepts / issues to be included in SLAs, often in the form of asking specific questions (Austria, Ireland), similar to the Gartner set-up (see *Draft suggestions for common terms of service and SLA's for cloud service contracts*.) They thus do not contain much detail on the description of actual service levels, such as the calculation of availability or compensation for non-compliance in the form of remedies. They could however act as guidance documents with regard to the issues which should be covered in our Model SLA.

## 3. LIST OF THE ESSENTIAL INFORMATION AND NECESSARY REGULATIONS THAT ARE IMPORTANT FOR DRAWING UP AND TERMINATING CSLAS

### 1.6. Development of the Model SLA – Stakeholder workshops and strategic considerations

The Model SLA can be found in the next section of this report. It was first developed by the Study Team in January 2015, on the basis of two principal inputs:

- The data from all Member States which was collected and analysed by the Study Team between January and June 2014. This data described the national legal framework, jurisprudence and policies in relation to cloud computing in general and SLAs in particular. The data collection also helped to identify comparable model clauses made available at the national level.

- Feedback collected through a workshop on 27 November 2014, during which suggestions from the user perspective were collected. The objective of this workshop was to find out which issues caused particular concern for cloud users, and thus which issues would benefit from the drafting of model clauses. Potential approaches for promotion and adoption of the Model SLA in the market were similarly discussed during this event.

After the initial development, the Model SLA was subsequently refined on the basis of feedback of the Study Team's Advisory Board, consisting of Profs. Thomas Hoeren, Christian Laux, and Paul Polański.

Finally, a third revision round (after the first workshop and suggestions from the Board) was organised through a second workshop, organised on 11 May 2015. Generally, the Model SLA itself was well received during this workshop, with specific appreciation for the explanatory comments, which were seen as beneficial to cloud users with limited resources or know-how. However, many participants also expressed doubts as to whether any model SLA text would be useful or appropriate in the current market: extensive customization would always be needed in practice, and the presentation of a single Model SLA document might erroneously suggest that a 'one size fits all' approach would be possible in the cloud market.

It was noted that an approach that would present the findings as a checklist or as a guidance document (rather than as a model SLA) would be equally useful and pose a smaller risk for confusion in the market. While the remit of this study was to produce a Model SLA – presented in the next section, updated in response to more specific

suggestions from the workshop – a checklist is therefore also included as Annex I to this report.

## 1.7.Key principles of the Model SLA

The Model SLA was drafted on the basis of certain key principles, which must be fully understood and respected in order to use the SLA correctly.

- Firstly, the Model SLA is **not a stand-alone contract**. It is intended to be appended to a main cloud services contract, which covers certain key aspects of the service, such as the identification of the parties, applicable law, jurisdiction, commercial terms, liabilities, and so forth. In that sense, the SLA is more properly understood as an annex to an agreement, than as an independent agreement.

- Secondly, the Model SLA is **cloud oriented**. While SLAs have a longstanding tradition in ICT contracts in general, this SLA is tailored towards the specificities of cloud computing, including its elastic on-demand self-service approach, and its use of multi-tenancy and resource pooling technologies[21].

- Thirdly, the Model SLA is focused on an **international context**. While it is drafted as a part of a study commissioned by the European Commission and considers European concerns and policy priorities (notably with respect to data protection), the clauses of the Model SLA do not assume that European law applies to the cloud service, nor that the parties are European citizens or companies. In this way, the Model SLA remains usable in an international context.

- Fourthly, the Model SLA focuses **only on measurable qualities** of the cloud service. This implies that each aspect (i.e. each service level objective) of the SLA must be expressed in the form of an obligation that can be evaluated objectively, and in which several tiers of service ('levels' in the sense of a service level agreements) can be comparatively identified and assessed. This does not necessarily imply that each service level objective must be expressed as a number; it may also be appropriate to use statements that can simply be evaluated as true or false.

- The Model SLA is drafted in a **technologically neutral** manner: all requirements are drafted in a functional manner without referencing the use

[21] For a more detailed description of these characteristics, see ISO/IEC 17788 'Cloud Computing Overview and Vocabulary'

of specific technologies. This ensures that the Model SLA can be used for all cloud use cases, and that innovation is not harmed or slowed because of restrictions imposed by the Model SLA.

- The Model SLA is similarly **business model neutral**: it makes no assumptions as to whether the cloud service is offered for free or against a fee, and whether the cloud provider has alternative sources of revenue than customer payments. It should be recognized however that some elements of an SLA may inherently be more appropriate for paid B2B use cases where the provider uniquely relies on customer fees. This is especially true when the customer's recourse consists of a discount towards the next invoice; such a recourse is meaningless if the customer does not pay to begin with.

- Finally, the Model SLA is **agnostic of the provisioning model**: it is equally appropriate for SaaS, PaaS, IaaS, or other cloud provisioning models. Similarly, the Model SLA is not targeted specifically towards public, private, hybrid or community clouds. It is however clear that the Model SLA is a contractual document, implying that cloud services are provided by (at least) one party to (at least) one other. For this reason, private cloud deployments where a single party manages its own cloud infrastructure will not benefit from the Model SLA, as there is no second party on which it can impose the obligations of the Model SLA[22].

Where necessary, the explanatory notes within the Model SLA will explain the impact of the principles on its provisions, thus also illustrating why certain choices have been made.

[22] In practice, many nuances can exist that impact the usability of the Model SLA. For instance, a cloud user might 'insource' cloud services, using internal infrastructure which is however managed/operated by a third party. Similarly, a public administration might use cloud services provided by a different public administration, which may a part of the same legal entity (e.g. a central government), or where both parties have no distinguishable interests. Whether the Model SLA is usable in such circumstances depends largely on the intent of the parties, and specifically whether they intend to create enforceable obligations from one party towards the other, or rather whether they wish to operate mainly on a best efforts/good faith basis.

## 1.8.Target audience and how to use the Model SLA

The Model SLA as included in section below is principally targeted toward professional cloud use cases (business to business or B2B use cases). While they may also be useful for consumer oriented cloud services (business to consumer or B2C use cases), they have not been drafted specifically with that context in mind. This is because the market characteristics and the resulting concerns are typically quite different: while B2B cloud services tend to be offered with a higher need and expectation with respect to the quality of services (which is also reflected in the fees paid by the users), B2C services tend to be less critical, and therefore have less of a need for SLAs. None the less, exceptions may exist, and the Model SLA may therefore also be useful to test whether a consumer oriented cloud service offers significant service assurances.

It is worth noting that the Model SLA is oriented towards both cloud providers and cloud users, without any specific preference or bias towards either user group. For cloud providers, the Model SLAs may be useful particularly as a source document on the basis of which they can create their own SLAs, or which they can use to test the adequacy of their existing SLAs. Similarly, for cloud users the Model SLA can be used as a starting point for any negotiations with cloud providers, or as a yardstick to assess the completeness and appropriateness of any SLA that is offered to them.

The Model SLA is of course particularly useful to providers or users with limited resources, in terms of time, financial means or know-how, as they might otherwise be unable to negotiate, draft or assess an appropriate SLA. The Model thus serves both a functional role – providing a template that can be used in practice – and a didactic role – showing users of the SLA which questions they should be addressing, and in what manner.

Finally, the Model SLA aims to serve the needs of the cloud computing community as a whole, irrespective of the cloud service model (SaaS, PaaS, IaaS, etc.) or business context. As was explained in the section above, this focus also implies that the Model cannot be used without tailoring or adjustment to the specific context, i.e. it is not a text that can be simply copied without modification.

In order to assist users of the Model SLA in this tailoring process, this document also contains explanatory notes, which have been integrated directly into the model SLA. The explanatory notes explain the purpose of each clause, and indicate potential pitfalls, concerns and dependencies. They can also propose alternative clauses that may be more suitable, depending on the service or context.

Furthermore, not all clauses will be appropriate for all cloud services. While the Model SLA is only a template that can be modified as needed by the users (implying that all

parts if it may be reviewed and changed or deleted as appropriate), some clauses are entirely optional and depend purely on the use case and business context. In these cases, the clause will be explicitly marked as ‘Optional’, and an explanatory note will explain why it is optional, and when it should or should not be retained.

Collectively, these notes aim to facilitate the correct and responsible use of the Model SLA in practice.

# 4. INPUT FOR THE DEVELOPMENT OF MODEL TERMS FOR CLOUD COMPUTING SERVICE LEVEL AGREEMENTS FOR CONTRACTS BETWEEN CLOUD PROVIDERS AND PROFESSIONAL CLOUD USERS - MODEL SLA

## 5.1. Preamble

The present document is a Service Level Agreement ('SLA'). It has been concluded in the context of an agreement which relates wholly or in part to cloud computing services (the 'Services Agreement'). The SLA has been appended to this Services Agreement and is referenced directly by the Services Agreement. The SLA applies to the cloud computing services and to the parties identified in the Services Agreement.

The party (or parties) that is required under the Services Agreement to provide cloud services will be referred to as the 'Cloud Service Provider' or 'CSP', whereas the party (or parties) that will be permitted under the Services Agreement to use such services will be referred to as the 'Customer'.

This SLA will define the specific service level objectives (SLOs) and service quality assurances which the CSP has committed to providing[23]. It also sets out any exceptions to these obligations, specifies measurement and evaluation procedures, and identifies any remedies to which the Customer is entitled. It should be noted that the obligations in the SLA relate to the services as described in the Services Agreement, irrespective of whether the CSP relies on a third party service providers to offer those services. Therefore, the obligations as set out herein shall include any service providers contracted by the CSP to offer the services to the Customer.

[23] For a more detailed explanation of these concepts, see the Cloud Service Level Agreement Standardisation Guidelines

***Explanatory note***

*The SLA is not a standalone document: it is intrinsically linked to a cloud services agreement. The scope of the agreement can actually be broader than mere cloud services; it may e.g. also including consultancy services, leasing or purchasing of hardware, etc. However, the SLA only applies to the cloud computing services, which should be explicitly described in the services agreement itself.*

*It is similarly possible that the Services Agreement applies to multiple cloud services, which may be covered by different SLAs. In this case, separate SLAs should be provided and referenced, which may or may not be based on the present Model SLA.*

*Note that the services agreement may consist of a single contract, or of a set of documents such as a basic services contract with relevant annexes (data processing agreements, security policies, etc., and of course the present SLA). The Services Agreement may take the form of general terms and conditions, including those published online (a paper document is not required), that apply to all customers of the cloud service.*

*Finally, as will be seen and explained in the sections further below, the Model SLA makes a distinction between service level objectives and service quality assurances. The former are traditionally found in most SLAs, and relate to business objectives that must be achieved by the CSP on penalty of a sanction (usually a discount). The latter is used in this text to identify service quality assurances which are linked to compliance: they must be achieved, and cannot be resolved by a discount.*

*By way of example:*

- *Availability is usually an SLO. If the service is insufficiently available, the customer may suffer business harm, and a discount might be an appropriate recourse.*
- *Data location however usually is not and SLO. If data is moved outside of a region that was approved by the customer, then this may raise significant compliance problems for the customer (and potentially also the CSP, depending on the case). Discounts are not an appropriate recourse for these issues.*

*A more pragmatic way of distinguishing between these two elements of the Model SLA is that the SLOs reflect a business need, whereas service quality assurances reflect a compliance need. In both cases, the Model SLA aims to strengthen transparency towards the customer.*

## 5.2. Definitions

The following definitions shall apply to the present SLA[24]. Insofar as these definitions contradict prior definitions provided in the Services Agreement for the same terms, the definitions below shall take precedence, but will only apply to the present SLA (and thus not to the Services Agreement itself, including any other annexes to the Services Agreement other than the present SLA).

- force majeure: any unforeseeable events that disrupt the execution of the Services Agreement, not within the control of either party to the Services Agreement, which cannot be overcome by the party who is in default of the Services Agreement by its exercise of due care
- remedy: compensation available to the Customer in the event the CSP fails to meet a specified service level
- service credit is a percentage discount offered to the Customer's next invoice in relation to the CSP's services covered by the present SLA in response to a breach of a service level objective
- service level objective: a specific, measurable characteristic of a cloud service for which the CSP makes a commitment
- metric: a standard of measurement that defines the conditions and the rules for performing the measurement and for understanding the results of a measurement

[24] Definitions have been taken from ISO/IEC CD 19086-1 (Information technology -- Cloud computing -- Service level agreement (SLA) framework and Technology -- Part 1: Overview and concepts) where available; see http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=67545. This standard was still under development at the time of drafting. Definitions are used in accordance with the ISO License Agreement, which notes that "Graphical symbols, terms and definitions, country, currency and language codes, whether they are part of a subscription or not, can be reproduced as needed for the implementation of these standards but they can't be resold." See http://www.iso.org/iso/home/store/licence_agreement.htm.

***Explanatory note***

*Definitions should be based on international standardized terminology wherever possible, to avoid regional or sectorial bias. The list above may be amended if appropriate and useful for the description of the further sections.*

*Users should be aware that the terminology used in this Model SLA has been aligned with the ISO/IEC CD 19086-1 draft standard in order to make it logically consistent, internationally usable, and as future-proof as possible. However, existing SLAs may use terminology differently, e.g. referring to each separate obligation as an 'SLA', rather than using this term for the contract as a whole. Care should be taken to ensure that terminology is unambiguous; it is with this objective in mind that these model terms use the ISO/IEC CD 19086-1 terminology wherever possible.*

## 5.3. Applicability and exceptions

The present SLA shall apply to the services as identified in the Services Agreement, and will remain in force for the same duration as the Services Agreement itself. When the Services Agreement terminates, the SLA shall similarly terminate automatically and without further notice.

The obligations as set out below will apply to all services as identified in the Services Agreement, and are legally binding upon the CSP. Any breaches of the obligations shall entitle the Customer to the remedies as set out below.

However, breaches of the SLA shall not entitle the Customer to any remedies if the CSP can demonstrate to the Customer that the breach was exclusively caused by a force majeure event.

Upon the condition that the event is unforeseeable for the CSP (including in terms of scope and impact), unavoidable and external to the CSP and that they make execution of the Services Agreement or the present SLA impossible, force majeure events include but are not limited to acts of God, acts of the public enemy, acts of terrorism, cyberattacks against any infrastructure used by or on behalf of the CSP to provide the services as identified in the Services Agreement, wars whether declared or not, blockades, insurrection, riots, epidemics, landslides, earthquakes, storms, lightning, floods, washouts, natural disasters in general, or civil disturbances.

Force majeure events shall not include any service outages or interruptions with CSP suppliers or subcontractors, with the exception of power or network outages that affect parties other than the CSP, its suppliers and subcontractors. Force majeure events shall also not include local incidents caused by the CSP or by CSP personnel (including local fires, local strikes, local labour disputes or unrests, or local industrial disturbances).

Furthermore, breaches of the SLA shall not entitle the Customer to any remedies if the CSP can demonstrate to the Customer that the breach was exclusively caused:

- By Customer's own hardware or software, including configuration errors or choices, hardware malfunctions or software bugs;
- By actions or omissions of the Customer or its agents, including Customer's choice not to follow usage guidance in relation to the CSP's services made available by the CSP, or by any actions or omissions of the Customer or its agents that violate any acceptable use policies that have been agreed between the CSP and the Customer;
- In relation to beta and trial services, provided that they have been identified as such to the Customer or its agents in advance by the CSP;
- By any actions or omissions of the Customer or its agents which are contrary to the Services Agreement or applicable law;
- By any actions or omissions of the Customer or its agents for which the Customer should reasonably have been aware that they would likely cause noncompliance with the provisions of the SLA.

Finally, the CSPs commitments under the SLA shall be suspended during any scheduled maintenance that has been communicated by the CSP to the Customer, either:

- Within or in accordance with the terms of the Services Agreement;
- Or using a communications channel that is habitually used between the parties, at least two working days in advance to the Customer.

If the total time of scheduled maintenance exceed 8 hours in a single calendar month, any hours in excess of 8 hours shall however be considered as being in breach of the SLA commitments.

In case of disputes with respect to scheduled maintenance, the CSP shall be required to prove that the maintenance has been communicated to the Customer in accordance with the requirements set out above.

The provisions of the SLA (including the exceptions are set out above) shall only apply insofar as they do not contradict applicable and binding law (including, as may be applicable, consumer protection legislation or legislation with respect to unfair contractual terms). If any of these provisions are found to contradict applicable and binding law, they shall be set aside without impacting the remainder of the SLA, and the parties will negotiate replacement provisions that most accurately reflect the parties' original intent insofar as this is possible without contradicting applicable and binding law.

***Explanatory note***

*The scope of applicability and exceptions are a key part of the SLA, and are among the most commercially sensitive aspects of an SLA. The draft above aims to strike a reasonable balance between the interests of the Customer and the CSP, and is based on various existing SLAs provided by CSPs operating in the European market.*

*Alternative provisions are possible and may be appropriate depending on the context. However, the following considerations should be kept in mind before varying any of the provisions above:*

- *The proposal above explicitly states that the service level objectives are legally binding. Some SLAs choose to describe the service level objectives as mere targets, non-binding KPIs, or best effort commitments, or as requiring the CSP to undertake commercially reasonable efforts to achieve the objectives. While this may be appropriate for some contracts, these clauses often imply that the Customer will have no legal recourse if the SLA is violated. This is generally not desirable for the customer, as it reduces the SLA to a non-enforceable statement of intent.*
- *Exceptions to the SLA are however virtually impossible to avoid, as absolute targets are often commercially or even technically infeasible. The list above is indicative, and parties may vary it as appropriate. However, the following exceptions are usually not desirable:*
    - *A generic Force Majeure exception without an explanatory statement of what this entails. The meaning and legal validity of such an exception may vary from country to country, making it unreliable from an international perspective.*
    - *Generic exceptions for all outages or service interruptions with any subcontractors. Cloud providers often rely on external service providers; if failures at their side are excluded entirely, this can remove much of the value of an SLA.*

***Explanatory note (continued)***

- *Exceptions for planned or unplanned outages or service interruptions without clear procedures to communicate them, as this essentially allows the CSP to disable the service entirely at will without breaching the SLA.*

*Finally, it should also be noted that the clause above lists examples of Force Majeure events that may not be appropriate for all cloud use cases. By way of example, a cloud user may opt to use a specific cloud service precisely because it is expected to provide protection against common cyberattacks (such as DDoS attacks), natural disasters or even wars. Inversely, the clause above excludes power or network outages that affect parties other than the CSP, its suppliers and subcontractors, e.g. national or regional outages which the CSP could not reasonably have prevented. However, this exception would not be appropriate for cloud contracts with international providers whose data centers are spread across the world with extensive fallback capacities, where even nationwide failures should not have an impact on the cloud service. In such cases, the clause should be updated to reflect reasonable expectations.*

*The model clause offers some protections on this point, as it requires that events are "unforeseeable for the CSP (including in terms of scope and impact), unavoidable and external" in order to qualify as Force Majeure. Foreseeable events such as relatively routine cyberattacks that any major provider suffers on a regular basis would not qualify as Force Majeure.*

*However, it is clear that there is always some margin of discussion as to whether the nature and scope of a cyberattack (or other possible event) is foreseeable to a CSP. Thus, if resilience is critically important to the user, it may be worthwhile to either remove these events from the list of potential Force Majeure events altogether, or at least to explicitly specify up to which point resilience is expected. On that point, it may be worth noting that section 2.10 contains several quality assurance statements that relate to resilience, redundancy, backups, recovery etc., all of which may be useful to resist or recover from incidents.*

## 1.9.Measurement and reporting of SLA compliance

Compliance with the SLOs specified in this SLA will be measured on a continuous basis by the CSP. The CSP shall either communicate any noncompliance with its obligations under the SLA proactively to the Customer using a communications channel that is habitually used between the parties; or alternatively it shall make an appropriate online interface available, free of charge, through which the Customer may verify actual performance of the CSP's services under this SLA over the most recently completed reporting period. The CSP may exclude from its measurements and reports any periods of time during which the SLA was suspended or for which the SLA did not apply, as set out in section 2.3 above.

Reporting periods have a duration of one month, i.e. the CSP must make any reports available on at least a monthly basis.

Upon the Customer's request, the CSP shall provide appropriate documentation to the Customer explaining in what manner SLA compliance is measured and reported via the aforementioned interface.

In case of disputes in relation to the measurement and reporting, disputes will be addressed in accordance with the general dispute resolution rules as set out in the Services Agreement.

***Explanatory note***

*Measurement is a key issue in relation to SLAs: stringent service level objectives are of little use if compliance is not properly measured or reported. The model clause above places this responsibility with the CSP, and requires it to make an online interface (i.e. a website, for instance a service management panel) available where the customer can check compliance over the most recent reporting period, set here at one month. While this is not currently a standard industry practice, the model clause includes it as a useful best practice which is in line with the self-service approach of cloud computing. There is of course nothing stopping the Customer from conducting its own measurements in whatever way it deems appropriate, but the measurement and reporting by the CSP should be taken as a default.*

*Many variations are possible. E.g. the reporting mechanism might use monthly status reports via e-mail instead of an online interface, and the reporting period can be set as longer or shorter as required. Similarly, it may be useful and possible to require separate or additional measurements and reports from the CSP's subcontractors. Whichever choices are made, it is crucial to ensure transparency on what is measured and in what way.*

*For the same reason – strengthening transparency - the clause above also allows the customer to ask for an explanation of how the CSP measures and reports its compliance, thus getting some insight into why the customer's experience may be different from the CSP's official reports.*

*The clause above does not contain specific redress mechanisms in case of disputes, and simply refers to the general rules of the Services Agreement (which may have an escalation process, or include arbitration/mediation, or may simply refer to a competent court). It is also possible to have alternative dispute rules in the SLA itself; this is however not often done in practice.*

## 1.10. Change management – revisions of the SLA

The provisions of the SLA may be revised by the CSP from time to time, as required by changes in the service provided by the CSP. Such changes will be considered to be accepted and legally binding to the parties, thus replacing the relevant provisions of the present SLA, on the following cumulative conditions:

- Changes in the SLA may never contradict any part of the Services Agreement or permit any non-compliance with any obligations under the Services Agreement or under applicable law.
- Changes in the SLA must be communicated at least one month in advance to the Customer using a communications channel that is habitually used between the parties.
- The Customer has the right to terminate the Services Agreement free of charge and without creating any right to compensation for the CSP if any communicated changes in the SLA will have or are reasonably likely to have a materially adverse effect on the Customer. The Customer must exercise this right within one month after being informed of the communicated changes; otherwise the Customer will be deemed to have accepted the changes.

The CSP shall ensure that an online archive is available to the Customer, free of charge, which the Customer can use to determine which version of the SLA was in force at any time while the Services Agreement is in force.

***Explanatory note***

*Change management, including unilateral changes which are implemented at the CSP's initiative, is not uncommon and not necessarily negative in cloud computing. Cloud computing services are usually more dynamic that non-cloud ICT services, which new features occasionally being added and old ones removed, affecting all customers. This may also have an impact on the SLA, which can improve or deteriorate over time.*

*This clause ensures that such changes are possible, and can be made on the sole initiative of the CSP. However, in such cases the Customer will have the right to terminate the Services Agreement as a whole if any chance is likely to be detrimental to the Customer. The provision thus tries to strike a balance between the CSP's need for flexibility and the Customer's need for predictability.*

*The clause above should not be used if stability is crucial to the Customer, or if the Customer has not obtained appropriate assurances with respect to exit modalities and data portability. In practical terms, the Customer's right to terminate the Services Agreement is of limited value if the Customer is unable to obtain a copy of its data or to migrate it to an alternative service provider.*

*Similarly, the clause above should not be used in cases where the unilateral termination right is an unacceptable business risk to the CSP (e.g. because it has sold services on the proviso that subscriptions would be paid for a longer period of time).*

*Finally, if the Services Agreement itself contains a change management clause, then it is advisable to align these. The clause above should not be used unless it is clear that the change management clause of the Services Agreement does not apply to this SLA.*

## 1.11. Breaches of the SLA

Breaches of the service levels set out in this SLA will entitle the Customer to a remedy as set out below, except in the situations defined in section 2.3 above.

***Breaches of service level objectives***

If a breach of a service level objective as stipulated below is measured and reported by the CSP, then the remedy will be provided automatically by the CSP. If the breach is not measured and reported by the CSP, then the Customer must demonstrate the breach to the CSP and claim the remedy using a communications channel that is habitually used between the parties. The claim must be received by the CSP within one month of the reporting period in which the breach took place. Breaches must be demonstrated by providing the CSP with any reasonable details regarding the claimed breach, including detailed descriptions of the claimed breach, its nature and duration, any causes that may be known to the customer, any attempts made by the Customer to manage, mitigate or resolve the Incident, and any technical information such as log files that could permit the CSP to assess the Customer's claim.

If the breach is found to be established, the Customer will be entitled to the service credits set out in the sections below. If more than one service level objective is not met in relation to the same incident, only the highest service credit shall apply (i.e. they shall not apply cumulatively).

The service credit applicable to each service level objective is set out below. If the Customer applies for the service credit or accepts it in relation to any breach of the service level objectives, then the Customer shall not be entitled to any other or additional compensation from the CSP in relation to that breach, nor to any other kind of recourse such as contract termination, except where required by binding applicable law.

Service credits are calculated at the end of each reporting period of one month, and on the basis of the amount paid during that reporting period. The credit will then be applied as a discount towards the following invoice that the CSP shall issue to the Customer in relation to the service covered by this SLA. If no future invoice is issued by the CSP to the Customer, then the Customer shall be entitled to a compensation payment equal to the credit accumulated during its last one month reporting period.

***Breaches of the service quality assurances***

If a breach of a service quality assurance as stipulated below is measured and reported by the CSP, then the CSP shall be required to provide notice of the breach to the Customer using a communications channel that is habitually used between the parties. The notice shall describe the nature and cause of the breach. The Customer is thereafter entitled to claim a remedy from the CSP in accordance with the provisions of the Services Agreement and taking into account any liability restrictions which may be set out therein. The breach shall however be qualified as a substantive breach of the Services Agreement.

***Disputes in relation to the SLA***

Any disputes in relation to the SLA will be governed by the same dispute resolution mechanisms (including the same applicable law and the same jurisdiction) as set out in the Services Agreement.

***Explanatory note***

*In accordance with industry practice, the breach clause above notes that breaches of service level objectives shall entitle the customer to service credits, i.e. discounts on future invoices. These should be granted automatically if the CSP detects them itself, or claimed by the Customer if the Customer identifies them.*

*Other mechanisms are conceivable as well, including flat rate payments to the Customer, coupons for other services or software, or free service boosts (e.g. additional storage space in the cloud); however, this is not customary. Credits are generally acceptable, provided that they are set at acceptable levels. Credits for each objective are set out in the sections below.*

*It is worth noting that the section above does not cumulate credits, but rather only selects the highest: if three objectives are breached in a month and each entitles the customer to a 25% credit, then the result is a 25% credit to the next invoice (rather than a 75% credit).*

*Finally, it should be noted that credits are only useful if a future invoice is still expected. If the Customer terminates a Services Agreement and the objectives are not met in the last month, then the provision above entitles the Customer to a compensation payment instead.*

*Similarly, service credits are not a useful mechanism for services provided free of charge. In such cases, SLAs are generally non-binding targets rather than enforceable commitments. This is not necessarily problematic, although the CSP should of course clearly communicate the non-binding nature of the SLA to the Customer.*

*It should also be noted that this can be a complex question in practice: is a 'freemium' service (where the basic package of services is free, but the customer may choose to buy upgraded service) to be considered as free? Or more ambiguously, one might consider the case where a customer buys hardware, but saves settings or use data in the cloud: in this case, the cloud service as such may be free, but the Customer may still rightly consider that their earlier payment included an economic consideration for the cloud service as well.*

*The Model SLA above assumes a monthly payment against which credits can be offset; this is the default commercial situation in cloud computing and is useful for most situations. Alternatives can be provided for the more ambiguous situations above; the main requirement remains that the CSP must be transparent on what assurances and remedies the Customer may or may not expect under the SLA.*

***Explanatory note (continued)***

*As noted above, the Model SLA also considers that some obligations cannot be dealt with satisfactorily through service targets and discounts. This relates to cases where the service obligation relates to an essential part of the service, i.e. an element without which the Customer would not have entered into the agreement, or may not even have been legally able to enter into the agreement due to compliance concerns. To address this issue, the Model SLA proposes a service quality statement in which service quality assurances are provided.*

*Breaches of a service quality statement should not give rise to a mere discount, considering that they are often substantive enough to cause significant compliance problems. Therefore, the Model SLA requires breaches to be qualified as material breaches, which give rise to the liability of the CSP as stipulated in the Services Agreement. It should be noted though that this liability may still be relatively limited, e.g. to the payments made over the last 6 months. This is however a commercial concern which the parties must examine as a part of their contractual diligence.*

## 1.12. Availability service level objective

The services covered by the present SLA shall be available to the Customer at least 99.9% of the time, evaluated on a monthly basis.

For the purposes of this SLA, the service shall be considered to be 'available' if it is capable of providing the services to the Customer in accordance with the description of the service as provided to the Customer by the CSP.

If the service level objective is not met, the following service credits shall apply (for the avoidance of doubt, only the highest credit in the table shall apply):

| **Measured availability percentage** | **Applicable service credit** |
|---|---|
| < 99.9% | 10% |
| < 99% | 25% |
| < 95% | 50% |
| < 90% | 100% |

***Explanatory note***

*Availability is likely the most common service level objective found in SLAs, but also very complex in practice, as 'availability' is very difficult to define and quantify. As this Model SLA aims to be applicable to all types of cloud services, the definition above is relatively broad and generic, describing it as being capable of providing the services as presented (e.g. through the Services Agreement, promotional materials, etc.).*

*Note that this objective only relates to the capability of the service: it is perfectly possible that the Customer wasn't able to use it in practice, e.g. because of network outages at the Customer's side; but actual use by the Customer is not a requirement for availability.*

*Wherever possible, the clause above should be phrased in a more specific and quantifiable manner. For instance, availability could be defined in terms of successful responses to requests/queries from the Customer, timely provisioning requests, response time, or even ability to maintain a certain capacity/data throughput at any given time. The more specific and quantifiable, the easier it will be to assess compliance.*

*The SLA could also be implemented and applied in a dynamic way, for instance through configuration panels that allow Customers to set desired targets through sliders on a control panel, thus setting new requirements for the future (and likely accepting the corresponding costs increase). Since this is however not currently an industry standard approach nor appropriate for all cloud use cases, the example clause above applies a more routine fixed target approach.*

*It is worth noting that the percentage applies to uptime over the month, without distinguishing e.g. office hours from night time, or working days from holidays, even though this might make a big difference in practice. If desired and appropriate, more specific definitions of the applicable timescale could be integrated.*

*It should also be noted that the model provision above is based on a 99.9% uptime baseline, which is close to industry standard. However, it foresees a very high credit of 100% (i.e. the next invoice is cancelled entirely) when availability is less than 90%, which can be considered strict and may not be appropriate for all contexts.*

## 1.13. Support service level objective

The support services as defined by the Services Agreements shall be offered in accordance with the service levels below.

For the purposes of this SLA, 'response time' refers to the duration of time between the submission of a support request by the Customer and the receipt of a substantive and non-automated response on behalf of the CSP (irrespective of whether the response resolves the issue reported by the Customer).

If no support requests are made, the objective will be automatically met.

| **Measured response time** | **Applicable service credit** |
|---|---|
| > 4 hours | 10% |
| > one business day | 25% |
| > three business days | 50% |

***Explanatory note***

*Some degree of support service is usually provided in cloud services, although the form may differ widely: access to FAQs, online forums, text chat, voice chat/telephone, contact forms, e-mail support, on-site support, etc. Different SLAs may be relevant, depending on the available support mechanisms.*

*The example above assumes a support mechanism whereby there is no instantaneous communication, and is thus e.g. appropriate for e-mail support or contact forms. For voice support or text chats, availability of a customer service representative (e.g. making someone available within 20 minutes) may be more appropriate.*

*The example above only relates to response times, and not to actual resolution; the former is relatively common in SLAs, whereas the latter is not. This is because resolution can be very complex and context specific, and it may therefore not be viable for a CSP to commit to any resolution targets in mass market cloud services, where the efforts required to resolve problems for a specific Customer may be significantly disproportionate to the service fee paid by that customer. Furthermore, for many cloud contracts, availability objectives will be adequate: if a problem is resolved, availability is resumed, and separate resolution objectives are therefore not useful.*

## 1.14. [Optional] Capacity service level objective

The services covered by the present SLA shall ensure that the Customer can simultaneously establish 100 connections at any given time during the reporting period, available to 50 individual users within the Customer's domain at any given time during the reporting period. Compliance with this objective is measured by determining if the service is able to provide the capacity requests made by the Customer when the service is available as defined above (i.e. during unavailability of the service as a whole, the capacity service level objective is not applicable).

If the service level objective is not met, the following service credits shall apply (for the avoidance of doubt, only the highest credit in the table shall apply):

| **Measured capacity** | **Applicable service credit** |
|---|---|
| < 100 connections *or* < 50 individual users | 10% |
| < 70 connections *or* < 35 individual users | 25% |
| < 20 connections *or* < 10 individual users | 50% |

***Explanatory note***

*Capacity is an optional service level objective in this Model SLA, as its viability and applicability is very context specific. The example above assumes that capacity can be usefully expressed in terms of numbers of connections to the cloud service and numbers of simultaneous users; these will be meaningless metrics to many cloud services. Alternative capacity indicators might be sustainable throughput, available resources (e.g. CPU clock cycles), simultaneous threads, etc. These examples are context specific, and in this case examining mainly IaaS use cases.*

*As with earlier provisions, the clause should be phrased in a specific and quantifiable manner wherever possible. It is also worth noting that the example above only applies the capacity objective if the service is available. This is to avoid claims of missing the capacity objective if the service is unavailable for even a few seconds, since this momentary interruption would immediately cause the highest penalty for the capacity objective (as no connections would be sustained during those seconds).*

## 1.15. Service quality assurances

The CSP shall ensure that its service is provided at all times in accordance with the service quality assurances marked in green in the table below.

| **Data Portability Quality Assurance (cells to be marked in green if applicable, red if not applicable)** | | | |
|---|---|---|---|
| Customer data is not retrievable by the Customer via a single download link or documented API interface. | Customer data is not available via the Internet; however, it is available via a physical carrier. | Customer data is retrievable by the Customer via a single download link or documented API interface. The data format is not documented in a manner that allows the Customer to understand the structure and semantic meaning of the data. | Customer data is retrievable by the Customer via a single download link or documented API interface. The data format is structured and documented in a sufficient manner to allow the Customer to re-use it or to restructure it into a different data format if desired. |

| **Data Location Assurance (cells to be marked in green if applicable, red if not applicable)** | | | |
|---|---|---|---|
| Customer data (included any copies or backups thereof) is stored exclusively in data centres | Customer data (included any copies or backups thereof) is not stored exclusively in data centres | Customer data (included any copies or backups thereof) is not stored exclusively in data centres | Customer data (included any copies or backups thereof) is not stored exclusively in data centres |

| | | | |
|---|---|---|---|
| physically located in an EU/EEA country, which are owned and operated by an entity established in the EU/EEA (including any data centres owned or operated by subcontractors of the CSP). | physically located in an EU/EEA country, which are owned and operated by an entity established in the EU/EEA. However, any processing and storage (including by subcontractors) is done in accordance with the requirements of approved EU Model Clauses[25] or in accordance with appropriate Binding Corporate Rules[26]. | physically located in an EU/EEA country, which are owned and operated by an entity established in the EU/EEA. However, appropriate legal measures have been taken to ensure that data can be lawfully stored in any data centres outside of the EU/EEA, taking into account the provisions of the Data Protection Directive 95/46/EC, if applicable. | physically located in an EU/EEA country, which are owned and operated by an entity established in the EU/EEA. However, appropriate legal measures have been taken to ensure the confidentiality and security of the Customer data, in accordance with the requirements of the Services Agreement. |

| **Security Certification Assurance (cells to be marked in green if applicable, red if not applicable; and to be completed as required)** | | |
|---|---|---|
| The services provided under the Services Agreement are certified at least annually by an independent auditor against a known security standard:<br><br>[Identify the relevant standard] | The services provided under the Services Agreement comply with a known security standard, but compliance is not verified by any third party:<br><br>[Identify the relevant standard] | The services provided under the Services Agreement comply with the security assurances which have been contractually agreed between the parties, but not with any known security standard. |

[25] See http://ec.europa.eu/justice/data-protection/document/international-transfers/transfer/index_en.htm

[26] See http://ec.europa.eu/justice/data-protection/document/international-transfers/binding-corporate-rules/index_en.htm

| | | |
|---|---|---|
| [Identify the relevant auditor] | | |

| **Encryption Assurance (cells to be marked in green if applicable, red if not applicable)** | | |
|---|---|---|
| The CSP does not provide any binding assurances with respect to encryption of Customer data. | The CSP will ensure that customer data will be encrypted whenever it is transported over a public communications network such as the Internet (both between Customer and CSP, and between data centres used by the CSP). | The CSP will ensure that customer data will be encrypted whenever it is at rest in data centres used by the CSP. |

| **Encryption Key Management Assurance (cells to be marked in green if applicable, red if not applicable)** | | |
|---|---|---|
| The CSP does not provide any binding assurances with respect to encryption key management as it applies to Customer data. | The CSP has implemented a key management policy which is applied and verified by the CSP. | The CSP has implemented a key management policy which is applied and verified by the CSP. The key management policy complies with the ISO/IEC27002 standard. |

| **Recovery Point Objective Assurance (cells to be marked in green if applicable, red if not applicable)** | | | | | |
|---|---|---|---|---|---|
| The CSP does not provide any binding | The CSP does not provide any binding | The CSP will ensure that recovery points | The CSP will ensure that recovery points | The CSP will ensure that recovery points | The CSP will ensure that recovery points |

| | | | | | |
|---|---|---|---|---|---|
| assurances with respect to recovery point objectives of Customer data: there is no guarantee that changes made to the Customer data can be restored. | assurances with respect to recovery point objectives of Customer data, but specific services or interfaces are provided to Customers to allow them to make backups at their own initiative. | are created for Customer data at least on a 7 day cycle. Customer data can always be restored, except for any changes made during the last 7 days. | are created for Customer data at least on a 24 hour cycle. Customer data can always be restored, except for any changes made during the last 24 hours. | are created for Customer data at least on an hourly cycle. Customer data can always be restored, except for any changes made during the last hour. | are created for Customer data on a continuous basis. Customer data can always be restored, and no changes made by the Customer will be lost except those made during a service interruption. |

| **Recovery Time Objective Assurance (cells to be marked in green if applicable, red if not applicable)** | | | |
|---|---|---|---|
| The CSP does not provide any binding assurances with respect to recovery time; there is no guarantee that service can be restored within a given timeframe. | The CSP will ensure that services provided to the Customer can be moved to a backup service if required with a recovery time of no more than 24 hours. The backup service will provide the same functionality and assurances as the CSP itself, and the switch can be made with the same | The CSP will ensure that services provided to the Customer can be moved to a backup service if required with a recovery time of no more than 1 hour. The backup service will provide the same functionality and assurances as the CSP itself, and the switch can be made with the same backup | The CSP will ensure that services provided to the Customer can be moved to a backup service instantaneously and continuously without noticeable service interruptions at the Customer side. The backup service will provide the same functionality and assurances as the CSP itself, |

| | | | |
|---|---|---|---|
| | backup assurances as the CSP itself (i.e. there will be no more data loss than in case of a backup restoration by the CSP itself. | assurances as the CSP itself (i.e. there will be no more data loss than in case of a backup restoration by the CSP itself. | and the switch can be made with the same backup assurances as the CSP itself (i.e. there will be no more data loss than in case of a backup restoration by the CSP itself. |

| **Personal Data Controllership Assurance (cells to be marked in green if applicable, red if not applicable)** | |
|---|---|
| When processing personal data within the context of the Services Agreement, the CSP will only act as a data processor in the sense of the Data Protection Directive 95/46/EC. | When processing personal data within the context of the Services Agreement, the CSP will act as a data controller in the sense of the Data Protection Directive 95/46/EC for at least some purposes. |

| **Personal Data Compliance Assurance (cells to be marked in green if applicable, red if not applicable; and to be completed as required)** | | |
|---|---|---|
| The services provided under the Services Agreement are certified at least annually by an independent auditor against a known data protection standard or Code of Conduct:<br><br>[Identify the relevant standard or Code of Conduct] | The services provided under the Services Agreement comply with a known data protection standard or Code of Conduct, but compliance is not verified by any third party:<br><br>[Identify the relevant standard or Code of Conduct] | The services provided under the Services Agreement comply with the data protection assurances which have been contractually agreed between the parties, but not with any known data protection standard. |

| | | |
|---|---|---|
| [Identify the relevant auditor] | | |

| **Data Deletion Assurance (cells to be marked in green if applicable, red if not applicable; and to be completed as required)** | | |
|---|---|---|
| The CSP does not provide any binding assurances with respect to the deletion of Customer data. | The CSP does will ensure that Customer data is effectively, irrevocably and permanently deleted (i.e. made inaccessible to anyone including the CSP itself without the use of data recovery techniques) whenever requested by the Customer, and in any case within one month after the termination of the Services Agreement. | The CSP does will ensure that Customer data is effectively, irrevocably and permanently destroyed in accordance with a known standard or technique (such as overwriting/data replacement standards and/or physical media destruction standards) whenever requested by the Customer, and in any case within 24 hours after the termination of the Services Agreement.<br><br>[Identify the relevant standard] |

| **Ecological Quality Assurance (cells to be marked in green if applicable, red if not applicable)** | | |
|---|---|---|
| The CSP procures all energy required for its data centres used under the Services Agreement from carbon neutral or renewable sources (including but not limited to geothermal power, wind power, hydropower, | The CSP has taken measures to ensure that the services provided under the Services Agreement are carbon neutral, and makes information available to the Customers to | The CSP publishes CO2-emissions generated by the data centres used under the Services Agreement, and publishes the methodology used by the CSP to determine these emissions |

| | | |
|---|---|---|
| and solar energy). | allow them to assess the basis for this claim. | and an assessment of their degree of accuracy. |

***Explanatory note***

*The table above contains samples of expected quality assurances that may be agreed between the parties. The tables are not exhaustive, and the parties can add additional qualities assurances where useful and relevant.*

*Contrary to the SLOs, there are no quantitative targets; rather, compliance can be assessed as a Boolean value: either the assurance is complied with, or it is not. As a result, no service credit mechanism is provided either: if the assurance is not provided, the Customer will be entitled to the recourse set out in the Services Agreement.*

*It is clear that the tables above only offer basic options with limited explanations. As such, they hide a great deal of complexity and details that may be extremely relevant in practice. E.g. the encryption assurance options say nothing about key management practices or key length and robustness of the algorithms being used. It is not suggested that the table is sufficient to replace contractual obligations or detailed policies. Rather, they serve to act as a quick transparency tool that can help Customers to get an easy (but therefore also imperfect and incomplete) overview of the key quality assurances that the CSP provides.*

*It should be noted that the obligations within a single Assurance topic are not necessarily mutually exclusive: multiple levels of assurance might apply, which would be indicated by multiple boxes being coloured in green. In this manner, the Model SLA allows Customers to quickly assess the assurances that a CSP provides. If applied consistently across a multitude of CSPs, the Model SLA could also be used for comparative purposes, verifying quickly which assurances different CSPs provide.*

# 5. RECOMMENDATIONS ON STRATEGY AND POLICY ASPECTS

## 1.16. Adoption and promotion

Based on the discussions of the two study workshops, several key recommendations for adoption and promotion were identified:

- Firstly, the general concern of participants in the broader workshop of 11 May 2015 should be repeated: there is a **desire for further consultation and development with stakeholders in the market**. Notably, stakeholders (particularly cloud providers) noted the sentiment that the systematic promotion of a single Model SLA might send an erroneous signal to the market, by suggesting that a one-size-fits-all approach is possible. Rather, it should be emphasized that the current Model SLA provides suitable building blocks for constructing an SLA, but that tailoring is at any rate needed for any cloud contract.

- Strategically, assuming that the Model has sufficient consensus and support, momentum could be created around the Model SLA by **leveraging an EU cluster of companies, focusing particularly on SMEs as a provider/user group** that has a significant benefit of model terms and a greater flexibility in adopting them. As was argued in the introductory sections above, parties with limited resources to dedicate on SLAs (both on the buyer and seller side of cloud computing) are a key demographic for model SLAs, as they arguably have the greatest benefit from model terms.

- Incentives for adoption could be created through **education and dissemination of the model**, and through **targeted promotion actions**. This has been done to some extent already by adding explanatory notes throughout the model above, so that users can identify some of the pitfalls and challenges in applying the model SLAs. Similarly, it was noted that it would be also be useful to examine if and how the enforcement / application of the model SLAs could be strengthened, e.g. through expedited and accessible dispute resolution schemes.

- More generally, the participants favoured a **bottom-up approach, focusing on SMEs**: targeting the SME-to-SME use cases, and thus create a sales target that could ultimately entice larger players to also address this market via the expected model SLAs. This bottom-up approach was seen as important to create trust and to ensure a sustainable support of an SLA model.

## 1.17. Further development of the Model SLA: a brief roadmap

Apart from these issues, several other recommendations have emerged in the course of the study, and notably in discussions with the Advisory Board, that could usefully be taken into account to further develop the Model SLA, thus also supporting its potential reach:

- Firstly, it has become clear that SLAs in cloud computing are the subject of significant standardization work, including within ISO, the NIST and the European C-SIG. This work has been referenced and built on in the model SLAs above to some extent. However, none of this work is completed yet. T**he Model SLA should be communicated to these initiatives, as it provides a useful example of how their work can be adopted, and may also indicate new potential areas of focus, such as through the distinction between traditional service level objectives and service quality assurances. In the same way, outputs of ISO, the NIST and the C-SIG should be reflected and integrated in the Model SLA**. This includes particularly the definition of appropriate metrics for SLAs (still largely ongoing in all of these initiatives), and the expansion and refinement of service level objectives and service quality assurances.

- Secondly, within the EU several cloud projects are ongoing that are producing SLA-relevant outputs, including **Cloud4Europe, SPECS, SLA READY, A4CLOUD, and SLALOM**. These projects could be **encouraged to re-use the Model SLAs and to revise/develop them further as needed**. This is not only useful as a mutually beneficial promotional activity, but also because some of these projects are actively developing the next stages of use for SLAs, including automated negotiation, comparison and evaluation of SLAs.

  The current Model SLA already provides a short preview of the form that this interaction could take. Specifically, the first six sections of the Model SLA (sections 2.1 through 2.6) are relatively stable, and could be applied as a standardized template, irrespective of the relevant SLOs or service quality assurances. The sections thereafter however (sections 2.7 and following) need to be tailored to the needs of each specific cloud contract. It is on this point that further standardization and development is most useful.

  One might image that these sections could be defined as dynamic interactive documents, e.g. as a semantically structured XML based document, in which only the required parameters need to be filled in by the CSPs that use the template. The resulting XML formatted SLA could then be applied in a semantically identical manner across all relevant service providers, thus enabling the aforementioned goals of projects are actively developing the next stages of use for SLAs, including automated negotiation, comparison and evaluation of SLAs. Essentially, this would imply making the current Model SLA machine readable and thus interoperable across multiple CSPs.

  This would significantly enhance the usefulness and business potential of the present Model SLA.

- Similarly, it could be usefully studied whether further variations of the Model SLA could be created that reflect various **tiers of service**. A simplified **quality classifications system** (e.g.

based on bronze, silver and gold level SLAs) might merit further study, as a way to reflect different needs of customers, and different service offerings in the market.

- Finally, the Model SLA should be **integrated with other still ongoing EU cloud related initiatives, including other C-SIG work on a data protection Code of Conduct[27], cloud certification[28] and SLAs[29], and ENISA's Cloud Certification Schemes List**[30]. These efforts can potentially be integrated into a unified scheme for trusted cloud computing, in which a single certification/attestation process could confirm the quality of service provided by any given cloud service. The inclusion of SLAs in such a framework, e.g. based on the present Model SLA, would significantly enhance the value of the work that has already been undertaken

[27] See https://ec.europa.eu/digital-agenda/en/cloud-select-industry-groupcode-conduct

[28] See https://ec.europa.eu/digital-agenda/en/cloud-select-industry-group-certification-schemes

[29] See https://ec.europa.eu/digital-agenda/en/cloud-select-industry-group-service-level-agreements

[30] See https://resilience.enisa.europa.eu/cloud-computing-certification

# 6. CONCLUSIONS

The present report has provided a template that can be used as a starting point for the creation and assessment of SLAs for cloud computing. The Model SLA was drafted taking into account the specificities of the cloud computing paradigm and of the European market, with its own specific legal framework and policy priorities. As such, it is a useful tool, particularly for stakeholders in the market with limited resources or know-how, particularly non-specialized SMEs.

The Study has however also observed that SLAs rely significant tailoring in practice, and that a one-size-fits-all approach is not feasible or desirable. For this reason, the study also provides explanatory comments which allow users to appreciate the meaning and relevance of each provision, and a checklist that can be useful to assess SLAs that differ from the model, perhaps in significant ways. In this way, the study outputs can be used even in cases when the Model SLA is not directly usable.

Finally, the Study has also provided recommendations for the promotion of the Model SLA, but also for its further development. On the latter point in particular, it is worth noting a number of highly innovative and ambitious EU projects that are studying possibilities for the automated negotiation, comparison and evaluation of SLAs. The Model SLA could be a relevant input for these studies. This would significantly enhance the usefulness and business potential of the Model.

Through these actions, the Study could contribute to achieving the objectives of the Digital Single Market, and could help the EU to take a leading position in the global cloud market.

## ANNEX I – CLOUD SLA CHECKLIST

The Model SLA as provided above can be used as a template to elaborate an appropriate SLA for a cloud service. However, it is important to note that some customization will normally be required to ensure that the result is appropriate for the specific service, and that it is suitable for both the CSP and the Customer.

The present section can be used as a checklist to determine whether an SLA – even an SLA that differs significantly from the Model SLA presented above – provides appropriate answers to the parties in a Services Agreement. The same structure has been applied as in the Model SLA, and for further detailed guidance and model clauses, we refer to the text of the Model SLA itself.

- Does the SLA **clearly identify the cloud service(s) to which it is linked?** Have you determined whether all the cloud services that you are procuring are covered (and if not: is this acceptable)?
- Is it clear whether the **SLA is legally binding, or is it merely a nonbinding statement of targets?**
- Does the SLA **clearly list any exceptions to its applicability**; i.e. does it describe what happens during scheduled maintenance, force majeure events, cybercrime attacks, etc.? Are the suppliers of the CSP also covered, or are they exempt? Is this acceptable for the present contract?
- Are **remedies clearly defined?** Are they effective as a deterrent and/or as compensation? If not, do you have other mechanisms to claim a compensation under the main Services Agreement?
- Is there a **clear list of commitments that the CSP will undertake?** Is it clear what each commitment means, what metrics are applied (i.e. what the criteria for determining compliance are), and how it is measured?
- Is it clear **who measures compliance with the commitments**?
- Is there a **reporting or monitoring mechanism to evaluate compliance with the commitments on a continuous basis?** This can be either passive (e.g. via a service management panel on a website) or active (e.g. via e-mail notifications).
- Does the **customer need to claim remedies in case of breaches, or will the CSP proactively offer the remedies?**
- Is there is **mechanism for resolving disputes,** i.e. is there a way to address any disagreements on whether the SLA was complied with or not? This can also be indicated in the Services Agreement rather than in the SLA.
- Can the CSP **unilaterally change the terms of the SLA?** Is this acceptable for this contract? It may also be advisable to check whether there are any clauses in the main Services

Agreement that allow the CSP to change the SLA. If the CSP may make changes to the SLA, then does the customer have access to an archive of prior versions?

- Is it clear **what happens if the Services Agreement is terminated while the customer is still entitled to a remedy?** Will the customer get a refund in these cases?

- **Are the commitments of the SLA appropriate for your Services Agreement?** For a more comprehensive list of potentially suitable commitments, you may wish to consult the Cloud Service Level Agreement Standardisation Guidelines[31]. Possible commitments include:

    - **Availability**
    - **Capacity**
    - **Support** (in terms of response and/or resolution)
    - **Reversibility and termination of the services**
    - **Service reliability**
    - **Cryptography**
    - **Security incident management**
    - **Logging and monitoring**
    - **Auditing and security verification**
    - **Data mirroring, backup and restoration, and data lifecycle**
    - **Data portability**
    - **Personal data protection / privacy protection**

[31] See Cloud Service Level Agreement Standardisation Guidelines

KK-01-15-509-EN-N

European Commission

# Standards terms and performance criteria in service level agreements for cloud computing services

Luxembourg, Publications Office of the European Union

**2015** – 78 pages

ISBN: 978-92-79-50117-3
DOI: 10.2759/07446

DOI: 10.2759/07446 ISBN: 978-92-79-50117-3