slalom

LEGAL & OPEN MODEL TERMS
FOR CLOUD SLA AND CONTRACTS

Final version

D2.2

Dissemination level: Public

Work Package	WP2, Legal Track
Due Date:	*M15 (31/03/2016)*
Submission Date:	*31/03/2016;*
Version:	*1.2*
Status	Final
Editor(s):	*Gian Marco Rinaldi (Bird & Bird)* *Debora Stella (Bird & Bird)*
Reviewer(s)	*David Bicket (CIF)* *Daniel Field (ATOS)*

The SLALOM Project is co-funded by the European Commission through the H2020 Programme under Grant Agreement 644720

Contents

Introduction

The purpose of this document is to provide a revised version of the legal model presented under the Deliverable D2.1 in the light of the recommendations that have been suggested by some stakeholders through their feedback. Moreover, this document is intended to reconsider some of the legal issues addressed in D2.1 due to the ongoing changes in the European legal framework occurring in the past few months, especially in the context of the Digital Single Market initiatives.

With reference to the feedback received by the stakeholders, we analysed the comments made by several different entities and organizations as well as natural persons, both on the Providers' side and the Adopters' side.

With reference to the changes occurred in the European legal framework, it is worth mentioning the political agreement reached by the EU Commission, Parliament and Council of Ministers during the "Trilogue" negotiation on December 15th, 2015[1] on the text of the General Data Protection Regulation that will replace the Directive 95/46/EC on the Protection of Personal data, and the invalidation of the EU-US Safe Harbor by the ECJ on October 6th, 2015 followed by the political agreement reached on February 2nd, 2016 between the EU Commission and the U.S. Department of Commerce on the new framework for transatlantic data flows with the EU-US Privacy Shield, which is still under scrutiny by the Article 29 Data Protection Working Party[2]. The recent speed-up of the work performed at the C-SIG level has also been taken consideration to further improve the legal assessment on the current status of development of market sensitivity to the standardization of service level agreements and the need to uniformly apply the data protection rules by cloud service providers.

This deliverable codifies fair terms and conditions for cloud services. This legal model is developed by SLALOM, a project funded by the European Union's Horizon 2020 research and innovation

[1] Draft of Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of data (2012/0011(COD)).

[2] It is worth mentioning the provisions included in the proposal for a directive on "Certain aspects concerning contracts for the supply of digital content" (COM (2015) 634 final) as they may also concern the cloud computing services offered to consumers. This proposal provides a definition of "digital content" as: "*(a) data which is produced and supplied in digital form, for example video, audio, applications, digital games and any other software, (b) a service allowing the creation, processing or storage of data in digital form, where such data is provided by the consumer, and (c) a service allowing sharing of and any other interaction with data in digital form provided by other users of the service*". The proposal set forth several measures of protection of the consumers in relation to the supply of digital content such as, among others, remedies in case of defects of digital contents or non-conformity with the contracts, provisions on the liability of the supplier, right of termination of the contracts, right to retrieve the content in case of termination or expiration of the contract.
Moreover, another proposal of directive has to be mentioned. It is the proposal for a directive concerning measures to ensure a high common level of network and information security across the Union (COM (2013) 48 final). Such proposal, among others, sets forth several obligations for the service providers (including the cloud computing service provider as per Annex II of the proposal) concerning the prevention, the handling of and the response to risks and incidents affecting networks and information systems. The cloud computing service providers shall be obligated to take appropriate technical and organisational measures to manage the risks posed to the security of the networks and information systems which they control and use in their operations and shall notify to the competent authority incidents having a significant impact on the security of the core services they provide, in line with the national legislations which will be implemented by each member state.

[2] Draft of Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of data (2012/0011(COD)).

programme under grant agreement No 644270.[3] There are a number of deliverables provided in this project, as listed in the references at the end. The inputs from the requirements deliverable have been taken into account in preparing the original version of this document.

The approach taken by this document is to discuss the main legal issues which impact on the relationship between a cloud provider (hereinafter, "Provider") and a cloud adopter (hereinafter, "Adopter"), and how such issues are generally provided for under contractual terms. Based on this discussion, proposals are then made for terms and conditions fair for both Providers and Adopters. It is not the purpose of this deliverable to describe the variety of cloud services available (SaaS, PaaS, IaaS, public, private, community or hybrid). It should be noted that the appropriate contractual terms for different types of services, and the appropriate balance of risk between the cloud Provider and the cloud Adopter, will vary according to on the nature of the services, the purposes for which they will be used and the pricing of those services (e.g. whether they are sold as premium services designed for the needs of a specific class of customer or as utility services available to a mass market). However, this deliverable discusses common areas of concern between cloud Providers and cloud Adopters and sets them within a contractual structure designed to provide a suitable model for contracting cloud services.

We will analyze the provisions that are generally included in an agreement for cloud services setting out the possible different interests, positions and perspectives of the two parties involved. This document primarily uses the term “Cloud Service Agreement” or “CSA” because the context of this document is cloud services.

We drafted the contractual provisions of the proposed SLALOM model CSA taking into consideration the legislation and regulations applicable to the relevant provisions in Italy, Germany, the UK, France and Greece. However, the nature of the services involved may affect the application of legislation and regulations and we have not comprehensively reviewed the legislation and regulations that are specific to certain industry sectors (e.g. financial services).

With reference to our analysis of the clauses used in the market, we examined several standard CSAs used by leading cloud service Providers which are available on the internet, and also agreements we have dealt with in the course of our professional activities. This document is not designed to evaluate the fairness or enforceability of the terms and conditions of the above CSAs as the said Providers draft their terms and conditions according to the specificities of their services and their internal operations and infrastructures. Furthermore, the terms and conditions of many Providers may also change as a result of negotiations with Adopters or due to the commercial relationships between the parties.

Following the feedback received on D2.1 during the consensus phase, we partially revised some of the SLALOM suggested provisions taking into consideration also the inputs so far received. A new

[3] SLALOM is an initiative aligned with the European Cloud Strategy. The first phase of the initiative is an 18-month, EC-funded project whose objective is to create a Service Level Agreement (SLA) reference model consisting of model contractual terms and model technical specifications. It seeks to provide clarity and reassurance to the market through establishing a baseline of fair and balanced provisions for cloud SLAs and cloud computing contracts overall. The initial members of the SLALOM consortium are global service provider ATOS (project lead), legal firm Bird & Bird (responsible for the legal track), the National Technical University of Athens (responsible for the technical track), the Cloud Industry Forum (responsible for the cloud service provider liaison track) and the University of Piraeus (responsible for the cloud Adopter liaison track). External collaborators and contributors are welcome. This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 644270.

paragraph was introduced at the beginning of each section of this D2.2 impacted by the changes to make easier the identification of the amended terms and conditions of the standard CSA.

Cloud Service Agreement

The Cloud Service Agreement or CSA is the main document which sets out the terms and conditions of the contractual relationship between the Provider and the Adopter in relation to the provision of cloud services.

As we are drafting a standard set of rules, we have not considered how this CSA will be concretely completed between the parties and we do not cover in this document possible legal issues deriving from the completion of the agreement, such as the application of legislation and regulations regarding e-commerce to the sale of cloud services.

The CSA is often executed via the internet especially in the case of a public cloud with standard terms and conditions.

In the case of customized services, or a contract specifically discussed by the parties, there more likely will be hardcopy contracts which are the final result of negotiations between the parties.

For ease of reference, the proposed SLALOM model CSA has "Attachments" in the same way as with a standard hardcopy agreement. In the event of execution via the internet, the contents of the Attachments can be provided in a specific document available online (e.g. through webpages linked to in the CSA).

The proposed SLALOM model CSA includes factors discussed in the sections of this document. For each section we will provide:

i) a general description of the subject matter of the clause,

ii) an analysis of similar standard clauses used on the market,

iii) the perspectives of the parties,

iv) the position proposed by SLALOM,

v) the Changes to the SLALOM proposed text after feedbacks ,

vi) the proposed text for that clause in the SLALOM model CSA.

The terms defined in Section 1 will only be used only in relation to proposed text in other sections.

Section 1: Definitions - Interpretations

General description of the section
This provision defines the meaning of the main terms used in a cloud computing agreement. They are important to clarify the intention of the parties in many of the areas covered later in this document.

Standard clauses used in the market.

Most of the general terms and conditions used in the cloud computing services market contain definitions of the terms employed in their provisions. No particular issues require comment in this respect.

With reference to the importance of having standardized definitions of technical terms see Deliverable 3.2 “SLA Specification and reference model – a”, Section 3.2.

Provider’s perspective	**Adopter’s perspective**
The Provider and the Adopter do not usually have any different perspectives on these provisions. Nonetheless, the meanings of some terms, when used in some specific provisions, can lead to very different interpretations of such provisions in favour of one or another of the parties. Therefore, the drafting of the definitions must take account of the effects they have on all the provisions of the cloud computing agreement in which they are used.	

Position proposed by SLALOM

Section 1 of the SLALOM model CSA will contain the list and meanings of all the main terms used in the CSA.

The definitions contained in this CSA are consistent with the definitions used in Deliverable 3.2 “SLA Specification and reference model – a” section 5 and Deliverable 4.1 “Initial Position Paper”, Section 3.

In accordance with the responses received to the SLALOM Questionnaire (Section 4.1), we have endeavoured to draft clear, simple definitions of the contractual terminology (as this is essential to ensure that the terms of the agreement are clear) which are as similar as possible to the technical definitions contained in ISO and C-SIG documents.

Changes to the SLALOM proposed text after feedback

i) We changed the name of the Agreement from "Master Service Agreement" in Cloud Service Agreement to make its subject matter clearer. This wording is provided, among others, by the ISO/IEC 19086 draft document on cloud computing services;

ii) we used the words "Adopter Data" in place of "Adopter Content" as these latter words seem to cover a wider range of information;

iii) we added "any applied discounts" (with reference to discount on the Charges) between the "Confidential Information";

iv) we simplified and reduced the definition of "Confidential Information";

v) in the definition of "Users" we included also "*other Third Parties authorized by the Adopter*". Accordingly, the Services, in addition to the employees, agents, consultants or subcontractors of the Adopter, could be used also by natural persons or entities external to the Adopter which may be authorized by the Adopter, provided that they are entitled to use the Services;

vi) we changed the "Working Days" so that it can apply to the widest range of countries (i.e.: we deleted Saturday and Sunday as fixed non- working days).

SLALOM proposed text

1.1 In this Cloud Service Agreement, unless otherwise stated or unless the context otherwise requires, each capitalised term will have the meaning set out below:

*1.1.1 "**Adopter**": the organization or natural person using the Services;*

*1.1.2 "**Adopter Data**": means any and all data, information and content which are i) uploaded, stored or installed by the Adopter onto the System or ii) created, realised or developed by the Adopter while using the Services, including, without limitations, data, information, software, data-base, documents, pictures, images, photographs, text, files, music, video;*

*1.1.3 "**Cloud Service Agreement**": means this agreement together with its Attachments under Section 23 below;*

*1.1.4 "**Confidential Information**": means any and all information or data, in whatever form or storage medium, whether tangible or intangible, and whether disclosed directly or indirectly before or after this Agreement by or on behalf of the disclosing Party (hereinafter, "Disclosing Party") to the receiving Party (hereinafter, "Receiving Party") in writing, orally, through visual means, or by the Receiving Party's evaluation, observation, analysis, inspection or other study of such information, data or knowledge, which is now or at any time after the Effective Date of this Agreement, owned or controlled by the Disclosing Party. Confidential Information shall include i) the Adopter Data; ii) the Charge due for the Services and any applied discount, and, iii) the trade secrets, discoveries, know how, designs, specifications, drawings, present or future products or services and markets, inventions, prototypes, algorithms, software of any kind or nature, object or machine codes, source codes, computer models and applications, developments, processes, formulae, technology, engineering, architectures, hardware configuration information, diagrams, data, computer programs, business activities and operations, customer lists, reports, studies and other technical and business information, and any other information which, by its nature, would reasonably be considered to be of a confidential nature either intrinsically or due to the context and circumstances in which it was disclosed, including, for the avoidance of doubt, information concerning the Parties' clients, which is of a confidential nature; iv) all the information under points iii) concerning or related to the Group of the Disclosing Party;*

*1.1.5 "**Charges**": means the charges due by the Adopter under Section 6;*

*1.1.6 "**Controller**" or "**Data Controller**": means the natural or legal person, public authority, organisation, agency or any other body which alone or jointly with others determines the purposes and means of the processing of Personal Data;*

*1.1.7 "**Data Protection Laws and Regulations**": means all applicable laws and*

regulations of the European Union (including the European Commission Data Protection Directive 95/46/EC[4], as amended or replaced from time to time), the European Economic Area and/or the relevant implementing law of any such member state (in particular the data protection legislation of the country where the Adopter is established to conducts the business to which the Services are related) and with respect to any other country, any applicable data protection or data privacy legislation;

*1.1.8 "**Data Subject**": means an identified or identifiable person to whom the Personal Data relate;*

*1.1.9 "**Documentation**": means all and any user guides and operating or other similar manuals and/or documentation, provided in hard copy or soft copy, necessary to enable the Adopter to make full and proper use of the System or the Service;*

*1.1.10 "**Effective Date**": means the date of enforcement of the Cloud Service Agreement, which is [to be inserted];*

*1.1.11 "**Force Majeure Event":** means any (i) fire, flood, earthquake or natural phenomena, (ii) war, embargo, riot, civil disorder, rebellion, revolution, which is beyond a Party's control, or any other causes beyond a Party's control;*

*1.1.12 "**Group**": in relation to each Party, means that Party, its subsidiaries, its holding companies and every subsidiary of each such holding company from time to time;*

*1.1.13 "**Intellectual Property Rights**": means all vested and future intellectual property rights including but not limited to copyright, trade-marks, design rights, patents, know-how, trade secrets, inventions, semiconductor topography rights, and any applications for the protection or registration of these rights and all renewals and extensions thereof existing in any part of the world, and all other intellectual property rights protected by any applicable law;*

*1.1.14 "**Party**": means the Adopter or the Provider;*

*1.1.15 "**Personal Data**": means any information relating to an identified or identifiable natural person (as defined under Directive 95/46/EC[5], as replaced from time to time, also known as Personal Identifiable Information under other legislations). This includes information that can be linked, directly or indirectly, to a natural person; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or using all means which can reasonably be used by the Data Controller or a Third Party to identify a natural person (e.g. one or more factors specific to his physical, physiological, mental, economic, cultural or social identity);*

[4] To be read as "General Data Protection Regulation" – GDPR – (the formal approval of the General Data Protection Regulation (2012/0011(COD)) is still pending at the date of release of this D2.2. This paper covers some of the main topics ruled under the GDPR (e.g. subcontracting, portability, personal data breaches and notifications, cooperation duties) relying on the text agreed at political level by the EU Commission, Parliament and Council of Ministers on 15th December 2015 Trilogue.

[5] See note no. 2.

*1.1.16 "**Processing of Personal Data**": means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;*

*1.1.17 "**Processor**" or "**Data Processor**": means the natural or legal person, public authority, agency or any other body which processes Personal Data on behalf of the Controller and according to its written instructions;*

*1.1.18 "**Provider**": means the organization providing the Service;*

*1.1.19 "**Provider Content**": means any and all content made available by the Provider to the Adopter onto the System, including, without limitations, data, information, software, data-base, documents, pictures, images, photographs, text, files, music, video;*

*1.1.20 "**Report":** means the report under Section 3.4;*

*1.1.21 "**Sales Tax**": means any applicable national, federal, state and local sales, use, value added, excise and other similar taxes, fees and surcharges that are legally or by custom borne by a purchaser of services;*

*1.1.22 "**Services**": means the services detailed in Attachment 1 to the Cloud Service Agreement, as such Attachment may be amended from time to time in accordance with this Cloud Service Agreement;*

*1.1.23 **"Service Credits":** means an amount in euro calculated each month in accordance with Attachment 2 in respect of a failure by the Provider to meet a Service Level Objective;*

*1.1.24 "**Service Levels**": means the characteristics of the Service defined under Attachment 2 to the Cloud Service Agreement;*

*1.1.25 "**Service Level Agreement**": means the Attachment 2 to the Cloud Service Agreement;*

*1.1.26 "**Service Level Objectives**": means the target numerical value of the Service Levels set out in Attachment 2 to the Cloud Service Agreement;*

*1.1.27 "**Subcontractor**": means any Third Party appointed by the Provider to perform some activities of the Services in accordance with Section 16.1;*

*1.1.28 "**System**": means the electronic information systems comprising any one or more of hardware, equipment, software, peripherals and communications networks owned, controlled, operated and/or used by the Provider to supply the Services;*

*1.1.29 "**Term**": means the term of the Cloud Service Agreement as specified under Section 9 of the Cloud Service Agreement;*

*1.1.30 "**Third Party"**: means any company, natural person, body or organization different*

from the Provider, the Adopter and the relevant Group;

*1.1.31 "**Third Party Content**": means any and all content owned by a Third Party made available or provided by the Provider to the Adopter onto the System including, without limitations, data, information, software (including open source software), data-base, documents, pictures, images, photographs, text, files, music, video;*

*1.1.32 "**Users**": means those employees, agents, subcontractors, consultants (including professional advisers) of the Adopter or other Third Parties authorized by the Adopter who are entitled to use the Service;*

*1.1.33 "**Working Days**": means any day which is not a [provide the day] or a bank or public holiday in [provide the Country].*

1.2 The following interpretation rules apply in this Cloud Service Agreement:

a) a person includes a natural person, corporate or unincorporated body (whether or not having separate legal personality);

b) the attachments form part of this Cloud Service Agreement and shall have effect as if set out in full in the body of this Cloud Service Agreement. Any reference to the Cloud Service Agreement includes the attachments;

c) a reference to a company shall include any company, corporation or other body corporate, wherever and however incorporated or established;

d) unless the context otherwise requires, words in the singular shall include the plural and in the plural shall include the singular;

e) a reference to a statute or statutory provision is a reference to it as it is in force as at the date of this Cloud Service Agreement;

f) a reference to a statute or statutory provision shall include all subordinate legislation made from time to time under that statute or statutory provision;

g) a reference to writing or written includes e-mail;

h) any obligation on a party not to do something includes an obligation not to allow that thing to be done;

i) a reference to this Cloud Service Agreement or to any other agreement or document referred to in this Cloud Service Agreement is a reference to this Cloud Service Agreement or such other agreement or document as varied or novated (in each case, other than in breach of the provisions of this Cloud Service Agreement) from time to time;

j) references to Sections and Attachments are to the sections and attachments of the Cloud Service Agreement or order (as applicable); references to paragraphs are to paragraphs of the relevant attachments;

k) any words following the terms including, include, in particular, for example or any similar expression shall be construed as illustrative and shall not limit the sense of

the preceding phrase. *1.3 If and to the extent of any conflict or inconsistency between the terms of this Cloud Service Agreement, the order of priority for the purposes of construction is, in descending order:* *a) the Sections of the Cloud Service Agreement;* *b) the Attachments under Section 23 of the Cloud Service Agreement; and* *c) the Annexes to any Attachment, if any.*

Section 2: Provision of services

General description of the section
This provision describes the subject matter of the Cloud Service Agreement and the main obligations. Therefore, first of all, such clause generally establishes that the Provider shall provide the services in accordance with the terms and conditions of the CSA[67]. In most cases, this clause will not provide a complete description of the services but will refer to a technical annex (or to a purchase form or to a webpage of their site), which will specify in detail which are the services to be provided.
Standard clauses used in the market
The cloud computing agreements of some Providers do not provide a clear obligation for the Providers to supply the services to the Adopter. The subject matter clause of such cloud computing agreements establishes instead an obligation for the Adopter to use the services in accordance with some specific rules and policies provided under the acceptable use policy. In some other cases, the agreements provide that the Provider "shall make available" the services to the Adopter. As many of such agreements are general terms and conditions not providing the special conditions of the services, they generally refer to the services detailed in the purchase order, in an attachment of the agreement or in other documents (e.g.: website pages) where the services are described.

[6] Under Italian law, a cloud computing agreement could be considered mainly a "service supply contract". Such general type of contract is provided under Article 1677 of Italian Civil Code - ICC providing that "*if the subject matter of the contract is the continuous or periodic performance of services, the provisions of this chapter* [i.e.: chapter on work contract, Article 1655 and followings of ICC], *and those relating to supply contracts* [i.e.: Article 1559 and followings] *apply, to the extent that they are compatible*". Some authors (Prosperetti), instead, qualify the cloud contracts mainly as "deposit contract" (provided by Article 1766 and followings of ICC). The different qualification implies the application of different rules to many profiles of the contract.

[7] From a German legal perspective, cloud services will typically qualify as “rental services”.

Provider's perspective	**Adopter's perspective**
The Provider could prefer not to establish a clear and precise obligation to provide the services focussing instead on the Adopters obligations relating the use of the services.	For the Adopter it is important that the Provider's obligations to provide the services are clearly expressed. Then, in case of default by the Provider in providing the services, the Adopter can easily refer to this provision when asserting its rights under the agreement.
Position proposed by SLALOM	
The main obligation of the Provider relating the provision of the Services should be set out in this clause but it should also provide that the Adopter may use the Services in accordance with the applicable terms and conditions established by the CSA (see also Section 5 below regarding the responsibilities that the Provider, as "provider of an information society service", might have in accordance with the provisions of Directive 2000/31). The Services shall be then defined in more detail in an attachment of the CSA (Attachment 1). Such attachment shall provide all technical details and specifications relating to the Services that the Provider undertakes to provide except for the Service Levels. The Services described in Attachment 1 shall be then linked to the Service Level Agreement provided in Attachment 2 of the CSA (see below)[8]. If the CSA is executed online, the Attachment 1 could be provided through a webpage of the Provider relating the Services. In this case, being such webpage under the exclusive control of the Provider, it will be advisable to provide whether the Provider has the power to unilaterally change the description of the Services.	
Changes to the SLALOM proposed text after feedbacks	
1) In Section 2.1, we replaced the wording "*The Provider shall provide the Services*" with "*The Provider shall make available the Services*" as this wording makes clear that, in most of the	

8 Under Greek law, cloud computing services would primarily qualify as information society services. Cloud providers would qualify as internet intermediaries that offer internet hosting services. Cloud services fall within various laws on ecommerce, copyright, consumer- and data protection, confidentiality of communications. Detailed legal evaluation relies on the type of public or private cloud offered. Depending on the type of Services provided ("Infrastructure as a Service- IaaS", "Platform as a Service -PaaS" and "Software as a Service- SaaS") a cloud contract may qualify as contract for works (Article 681 Civil Code), lease (of network capacity or storage space) (Article 574-612 of Greek Civil Code), sale of goods (including services) (Article 513 – 571 of Greek Civil Code) and so on. The particular Provider and Adopter rights and obligations regarding contract conclusion, faulty performance, parties' rights, price, remedies, withdrawal, suspension or termination of service, indemnification, renewal, governing law and jurisdiction etc. depend to a large extent on the contract qualification. Moreover, additional rules may apply under Greek law such as tax – related storage requirements for IaaS, electronic invoicing rules or electronic signatures for SaaS services, copyright law 2121/1993 on protected works with the private copying exception also been applicable on CSPs for private but not for public use of cloud data. Cloud providers in principle do not constitute publicly available communications services (under P.D. 47/2005) therefore they may exceptionally be obliged to grant access to ordinary cloud data to law enforcement by virtue of a relevant Public Prosecutor Order on ground of criminal investigation. Access to cloud data can in principle be granted by local providers to foreign enforcement authorities, further to relevant disclosure requests made on the basis of a Mutual Legal Assistance Treaty (MLAT), which allow generally for the exchange of admissible evidence and information in criminal matters.

cases, the Services are made available for the use of the Adopter and are not unilaterally provided by the Provider regardless of the effective use of the Adopter. The use by Adopter of the Services then has to comply with the Acceptable Use Policy under Attachment 3. The structure of Section 2 should better represent now the usual operating of most cloud computing services.
SLALOM proposed text
2.1 The Provider shall make available the Services to the Adopter from the Effective Date, in accordance with the Service Level Agreement in Attachment 2 and the other terms and conditions of the Cloud Service Agreement. *2.2 The Adopter shall have the right to use the Services in accordance with the Acceptable Use Policy under Attachment 3 and the other terms and conditions of the Cloud Service Agreement.*

Section 3: Service levels

General description of the section
In cloud computing agreements, this clause requires the Provider to supply the services in accordance with certain service levels agreed between the parties and in accordance with the service level objective[9]. The service levels define the quantitative and qualitative characteristics of the services[10]. As it is not possible to include all such technical details within the clause of the agreement, the clause generally refers to an attachment which with reference to the agreement executed online is provided in a separate webpage of the Provider. Such attachment will provide parameters and formulas to measure the performance of the Provider in relation to services described by the agreement. The service levels shall also be connected with the service credits provisions which are triggered by the breach of the SLAs[11].
Standard clauses used in the market
Cloud computing agreements generally provide a section relating the service levels. Where such agreements are executed via the internet, such sections usually refer to some webpages providing the details of the service levels. For an in-depth analysis of the service level agreements provided by some cloud computing agreements, please see Section 3.3. of Deliverable 3.2 “SLA Specification and Reference model a”. It is worth stressing that some cloud computing agreements establish that the Provider may

[9] Communication COM(2012) 529, Unleashing the Potential of Cloud Computing in Europe, page 11; European Commission's Expert Group Document, Availability, pag. 1; W. Kuan Hon, Christopher Millard & Ian Walden, *Negotiating Cloud Contracts: looking at clouds from both sides now, Stanford Technology Law Review. Volume 16*, Number 1 Fall 2012, pag. 97.

[10] Dimosthenis Kyriazis, *Cloud Computing Service Levels Agreements, Exploitation of Service Level Results.*

[11] Judith M. Myerson, *Best Practises to Develop SLAs for cloud computing*, IBM Corporation 2013.

unilaterally change or update the service level agreement.

Many cloud computing agreements do not specify how possible violations of the service level agreement are communicated or shared with the Adopter.

It is common providing that the only remedy provided for the breach of the SLA is the application of service credits.

The above mentioned cloud computing agreements provide for several cases of exclusion of the SLA. For instance, in all cases of force majeure; in case the breach depends on the performance or non-performance of some activities by the Adopter or a third party; in case of breach of the SLA deriving from Adopter's use of hardware or software not provided by the provider; in case of failure deriving from the maintenance of the provider's systems; in relation to beta version of its products; in case of errors resulting from abuses; or in case of use of the services not in line with the guidelines provided by the provider.

The general terms and conditions of some cloud services provided for free do not contain any service level agreement.

Provider's perspective	**Adopter's perspective**
From the perspective of the Provider, as a first choice, it would be preferable to have a generic reference to the quality of the services rather than providing numeric parameters to fulfil. As a second option, if the parties agree to stipulate service levels, the Provider is more likely to prefer that the standards they are required to operate to, in respect of the service level agreement, are subject to a "reasonable commercial effort" or a "best effort" instead of a precise obligation to respect them. However, in many cases, the Provider is likely to accept service level if it can provide the payment of (not high) service credits is the sole and exclusive remedy for the Adopter in case of breach of the SLA by the Provider.	The Adopter is interested in establishing that the Provider must adhere to the service levels so that where the Provider fails to fulfil one or more of them in a certain amount of time, the Adopter shall be entitled to ask for the application of service credits, the payment of penalties, or the termination of the cloud computing agreement. The Adopter will therefore want to specify detailed service levels and service level objectives which concern all important topics of the Services and which can be verified objectively. The Adopter is interested in monitoring all activities performed by the Provider and all details of the services as the application of possible penalties or service credits depends on such information. Therefore, the Adopter needs to receive periodical (monthly if possible) reports on possible violations of SLA.

Position proposed by SLALOM

The Parties shall set out clear and measurable technical conditions of Service delivery in order to make the services comparable with the services provided by other vendors, the Service Levels should be construed in line with service levels generally used by other vendors for the same activities.

It is not advisable to specify a "best effort" (or similar language) to meet the SLA because this kind of provision does not make it clear or certain whether specific SLAs have to be fulfilled or not. In

addition, the Provider can avoid fulfilling certain SLAs by arguing that, despite its best effort, it was not possible to achieve them. It is therefore advisable to agree an obligation to fulfil SLAs which have been carefully determined and which can be (wherever possible) periodically adjusted by agreement of the Parties.

The Provider should also be required to provide, or make available on the Service website, a periodical report which makes clear to the parties whether possible violations occurred (see on this point Deliverable 4.1/5.1 "Initial Position Paper", Section 4.9.3). This document shall be issued by the Provider and the parties shall apply the possible Service Credits on the basis of this document.

We provided also the possibility for the Parties to review the SLA. Actually this provision is likely not acceptable to public cloud Providers which have the same SLA for all their customers and are generally not available to periodically discuss them with the customers.

Changes to the SLALOM proposed text after feedbacks

1) We added an optional clause providing a continuous reporting (allowing an ongoing monitoring of the Services by the Adopter) instead of a periodical report sent or made available by the Provider;

2) we added on optional clause providing the right of the Adopter to have an audit made by an external independent auditor relating the Service Levels and their compliance with the data and information provided by the Provider with the Report.

SLALOM proposed text

3.1 The Provider shall provide the Services in accordance with the Service Levels under Attachment 2 to this Cloud Service Agreement.

3.2 Where the Provider fails to fulfil the Service Level Objectives during the Term of the Cloud Service Agreement, Section 7 below shall apply.

3.3 Without prejudice to any possible rights, remedies and/or actions of the Adopter in accordance with applicable law or this Cloud Service Agreement, the Provider shall inform the Adopter, as soon as reasonably practicable, of any anticipated failure to meet any Service Level Objective and of the steps that the Provider will take (or has already taken) to prevent the failure from occurring.

3.4 Within [to be inserted] ([to be inserted]) days after the end of each month during the Term of the Cloud Service Agreement, the Provider shall provide or make available to the Adopter a Report including the following information:

a) applicable Service Levels;

b) Service Levels Objective accomplished;

c) Service Levels Objective not-accomplished;

d) application of possible Service Credits, in accordance with Section 7.1 of this Cloud Service Agreement.

[ALTERNATIVE - 3.4

3.4 The Adopter shall be entitled to remotely monitor the ongoing performance of the Services having the rights to access, on a continuous basis, a Report providing the following information:

a) applicable Service Levels;

b) Service Levels Objective accomplished;

c) Service Levels Objective not-accomplished;

d) application of possible Service Credits, in accordance with Section 7.1 of this Cloud Service Agreement].

[OPTIONAL 3.5 During the Term of the Agreement and for a period of 3 (three) months following its termination or expiration, the Adopter has the right, at its expense, to have the Provider data and information relating the performance of the Services inspected by an independent auditor (the "Auditor") appointed by the Adopter, who shall be approved by the Provider (and such approval cannot be unreasonably withheld), so as to verify compliance by the Provider with the Report provided or made available. The Provider shall render all necessary assistance and cooperation to facilitate such inspection and shall make available to the Auditor exclusively all relevant files, data and information used to determine the Service Levels and shall instruct its employees to act accordingly. The Auditor shall communicate promptly to the Adopter the findings and results of his audit. The Auditor shall not communicate to the Adopter any Confidential Information resulting from the performance of his audit but shall only notify the Parties, if or if not, his audit concludes to different Service Levels Objectives than the ones communicated in the Reports. In the event of an audit result that shows a discrepancy of more than 5% (five-per-cent) to the detriment of the Adopter, the Provider shall bear the full costs invoiced by the Auditor.]

[OPTIONAL: 3.6 The Parties shall meet 30 (thirty) days before the end of each year during the Term to review the Service Levels and the Service Level Objectives. During the review, the Parties shall examine the Reports provided by the Provider during the year in accordance with above Section 3.4. Where one Party proposes to change the Service Levels and Service Level Objectives, the other Party shall not unreasonably deny its consent to such change].

Section 4: Variation of the services

General description of the section
This clause concerns the possible variation of the services to be provided. Such change can normally derive from: i) external causes (including the case of change of circumstances affecting the services, change of the legislation or order of the authorities having effect on the services); ii) request of the Provider; iii) request of the Adopter[12]. It could be important to provide a process

[12] In the work contract type under the Italian Civil Code - ICC (i.e.:"Contratto di Appalto", which relates to realization of works and, together with Article 1559 c.c. and followings, to the extent they are applicable, the supply of services), the possibility to change the work or the services is provided under Articles 1659-1661 ICC.

governing this variation so that in case this request of variation occurs, the parties already know how to manage it and the contract relationship is not affected or endangered in any way[13]. Moreover, it would be easier to implement the provision of additional service or content in favour of the Adopter.

In case of changes unilaterally set out by the Provider, some experts argue that the right of termination of the Adopter will be granted especially if above changes have been implemented by the Provider and have an impact on:

- the financial terms applicable between the parties;
- terms regarding data processing, security, localization;
- more generally, any term which modification may impact Adopter's costs in using the applicable Services.

In contract with consumers, according to Directive 93/13/EEC (Annex 1, (point k)), the unilateral alteration of the services without a valid reason is considered as an unfair term. Therefore, if not specifically negotiated by the parties, a clause including above unilateral right of variation could be considered as void[14].

Under Greek consumer law[15], the transparency and control of fairness of terms is of paramount importance. As a general rule, Greek courts tend to consider null and void unfair contractual terms, such as the unilateral variation of the services by the Provider, by protecting the consumer that is generally at a disadvantage compared to the specialist such as a cloud Provider.

Standard clauses used in the market

Especially in relation to public cloud services, it is common establishing that the service, as well as SLAs, or other profiles and details of the contractual relationship with the Adopter (including the terms and conditions of the cloud computer agreement itself) may be unilaterally changed by the Provider without any approval of the Adopter.

Such changes generally do not need to be justified by the Provider which can implement them at its discretion without being obligated to provide the reasons of such change.

In some cases, it is not clear if and how such changes are communicated to the Adopter.

In most of the cases, the Adopter does not have the right to withdraw from the cloud computing

Some authors think that such articles are applicable exclusively to the realization of works but not to the supply of services. In any case, the parties are free to contractually regulate this profile of their relationship.

[13] Federico Tosi, *Il Contratto di Outsourcing di Sistema Informatico*, Giuffré, pag. 67; Alessandro Musella, *Il Contratto di Outsourcing di sistema informativo*, Diritto dell'informazione e dell'Informatica, 1998, pag. 867; Zincone, *Il Contratto di Outsourcing: natura, caratteristiche, effetti*, Rivista Dir. Autore 4/2002, pag. 392.

[14] This provision of the Directive 93/13/EEC has been implemented in Italy under Article 33, para 1, sub-para m) of the Code of Consumers (Legislative Decree 206/2005).

[15] Consumer protection Law No. 2251/1994, as amended, which regulates several aspects of remote business to consumer (B2C) and business to business (B2B) contracts, by implementing various EU Directives (e.g. Directive 1999/44/EC on Consumer Sales, Directive 93/13/EEC on Unfair Terms in Consumer Contracts, Directive 2005/29/EC, transposed through Law 3587/2007, prohibiting unfair commercial practices etc.).

<table>
<tr><td colspan="2">agreement in case of changes to the services by the Adopter.</td></tr>
<tr><td>Provider’s perspective</td><td>Adopter’s perspective</td></tr>
<tr><td>Depending on the nature of the services, the Provider will be concerned to ensure that:

i) the scope of the services are established at the execution of the cloud computing agreement and cannot be modified or integrated with other systems unless the parties agree on the possible integration and the consequences (financial or operational); and/or

ii) make bug fixes and security patches whenever required; and/or

iii) it has complete discretion to unilaterally develop the services including adding, removing or modifying functionality.</td><td>The Adopter will be concerned to ensure that:

i) the services can be changed upon request of the Adopter;

ii) the Provider will update the services to remain compliant with any changes in applicable law;

iii) the Provider cannot change the services unilaterally, especially where such change results in the removal of functionality or changes to the legal rights or obligations of the parties;

iv) where the Adopter has requested a change in the services in accordance with i) above the fees payable by the Adopter will not increase unless the Provider can demonstrate by way of an impact assessment that, as a result of the Adopter's request, the Provider will incur a substantial increase in the amount of expenses and resources required to effect such request;

v) where the provider insists on the unilateral right to change the services by the provider, the Adopter will request the right to terminate the CSA.</td></tr>
<tr><td colspan="2">Position proposed by SLALOM</td></tr>
<tr><td colspan="2">Further to the feedbacks received on this Section, we decided to provide significant changes to the relevant provisions.

As the services are very often updated and improved by the providers, the proposed SLALOM model CSA states that the Provider will be entitled to change the services provided that such changes do not determine in any way a reduction of the functionalities or characteristics of the services as they were offered at the effective date of the agreement. If the Provider wishes to reduce the functionalities and characteristics of the services, such changes need to be approved in writing.

As an exception of the above provision, the Provider will be entitled to improve or update the Services in case of improvements or updates necessary to fix defects of the Services or to cure security vulnerabilities of the System (as suggested the DG Justice Group experts, see Deliverable 4.1, Section 4.3); and in case of new laws, regulations acts or orders of the authorities which</td></tr>
</table>

require changes to the Services. In all these cases, however, if the changes provoke a reduction of the functionalities or characteristics of the Services, the parties must agree a fair and proportionate reduction of the due charges.

We preferred not to provide the right of termination for the Adopter (as suggested by ECP C-SIG group and the CSCC guide, see Section 4.3 of Deliverable 4.1 “Initial Position Paper”) in case of changes by the Provider as in many cases this seems not a feasible remedy for the Adopter which could be not in the position to easily change Provider.

As optional clause, which would likely be not applicable for standard services of public cloud Providers, in case of request of variation of the Services by the Adopter, the Provider shall provide the Adopter within a specified deadline an estimate of any potential increases in the consideration due (e.g. fees etc.) together with the potential impact on the delivery and use of the Services and on the applicable Service Levels.

Changes to the SLALOM proposed text after feedbacks

1) This Section has been redrafted as explained in the above paragraph "Position proposed by SLALOM".

SLALOM proposed text

4.1 Without prejudice of following Section 4.2, the Provider shall be entitled to change the Services during the Term unless such changes determine, directly or indirectly, a reduction of the functionalities or characteristics of the Services as originally provided at the Effective Date. Save for the changes under Section 4.2 of the Cloud Service Agreement, any change to the Services determining, directly or indirectly, a reduction of the functionalities or characteristics of the Services must be agreed in writing by the Parties.

4.2 The Provider shall be entitled at any time to improve or update the Services in case of: i) improvements or updates necessary to fix defects, bugs, malfunctioning or errors of the Services; and/or ii) to cure security vulnerabilities of the System; and/or ii) the application of any new laws, regulations acts or orders of the authorities. In case the changes under this Section 4.2 determine, directly or indirectly, a reduction of the functionalities or characteristics of the Services as originally provided at the Effective Date, the Parties shall agree a fair and proportionate reduction of the due Charges.

[OPTIONAL 4.3 The Adopter shall have the right to request a change to the Service by notifying to the Provider the requested change ("Change Request"). The Provider shall respond to the Change Request within [10 (ten)] working days or such period as agreed between the Parties by submitting a written response outlining the reasons for non-acceptance or agreeing to the Change Request by a specified time together with any terms of acceptance, including a quotation for implementation of the Change Request and any potential impact on the Charges, the performance and use of the Services and on the Service Levels. Where the Provider's response requires greater understanding and discussion of the Change Request both Parties agree to deal with the matter in an expeditious and timely manner].

[OPTIONAL 4.4 Changes to the Services under above Section 4.3 shall only have validity where the authorised representatives of both Parties have agreed and signed a change order

(hereinafter, "Change Order"). Following the signature by both Parties of a Change Order, this Cloud Service Agreement shall be amended to include the Services and any other terms as amended by the Change Order].

Section 5: Obligations of the Adopter

General description of the section

This clause may provide both: i) the terms and conditions that the Adopter has to respect while using the services[16], as well as ii) possible activities that the Adopter has to perform to allow the Provider to supply the services (e.g.: provision of data, information or documentation).

As it is normally not possible to include the above terms and conditions in one clause of the cloud computing agreement, this clause refers to an external document commonly called the AUP (Acceptable Use Policy) which details all obligations of the Adopter in relation to the use of the services.

It is worth noting that, in accordance with Directive 2000/31/EC (implemented in the EU member States)[17], the Provider "*is not liable for the information stored at the request of a recipient of the service, on condition that:*

(a) the Provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or

(b) the Provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information".

In light of the above, if the Adopter violates the law or any third party rights with the content uploaded on the cloud, and the Provider is aware of such violations, the Provider is obligated to act to stop such violation.

From a contractual point of view, it is important to provide the Provider with all contractual means to enable it to comply with the law.

Under French law[18], the Provider hosting content through cloud services will be subject to a "notice and take down" obligation substantially in line with the requirements set forth by Directive 2000/31/EC. In this respect, the Provider will not be held liable, either from a civil or criminal standpoint, in respect of any content or information hosted on its systems unless the Provider can establish that:

[16]European Commission, *Comparative Study On Cloud Computing Contracts, Final Report*, March 2015, pag. 36; Kuan Hon, Christopher Millard & Ian Walden, *Negotiating Cloud Contracts: looking at clouds from both sides now, Stanford Technology Law Review. Volume 16*, Number 1 Fall 2012, pag. 123; Eugenio Prosperetti, *Diritto dell'Internet*, Cedam, edited by Giuseppe Cassano, Guido Scorza, Giuseppe Vaciago pag. 689.

[17]Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce')

[18] Artt. 6-I-2°, 6-I-3° and 6-I-5°of the law for confidence in the digital economy *(« Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique* » or « LCEN »)

(i) it had actual knowledge of the unlawful nature of such information or content or

(ii) from the moment it was notified of the unlawful nature of such information or content, it did not act promptly to remove them or make them otherwise unavailable.

Standard clauses used in the market

Most cloud computing agreements provide an "Acceptable Use Policy". As stated above, such policy establishes the terms and conditions to be respected by the Adopters while using the services.

The above policies generally forbid using the services, by way of example:

i) in relation to upload, creation or distribution of illegal content;

ii) to perform illegal activities;

iii) to perform security violations, both in the network, computer or electronic systems of the Provider and/or third party;

iv) to violate the rights of third parties;

v) to distribute viruses, Trojan horses, worms, malware or similar applications; or

vi) to distribute or publish unsolicited emails, advertising or promotions.

Some Providers do not clearly establish the consequences of the breach of the AUP by the Adopter. In other cases, they provide the possible suspension of the services or even the termination of the cloud computing agreement.

Some Providers specify that they may report to the competent authorities (or also to third parties in general) any activity that they suspect violates the laws and that they will cooperate with such authorities.

Sometimes, the cloud computing agreement even provides that the Adopter shall indemnify the Provider for costs or damages arising as a result of any violation of the Acceptable Use Policy by the Adopter.

Provider's perspective	**Adopter's perspective**
The Provider's concern is to ensure that the Adopter follows the terms and conditions of use of the services as provided in the AUP also considering the possible consequences and damages that the Provider could suffer for the breach of the law or third parties' rights by the Adopter while using the services. The Provider will also be concerned by any act or content that, though not illegal, might negatively impact the performance of the	The Adopter would prefer not to have obligations regarding use of the services or to refer broadly to the respect of all applicable law and regulations. The Adopter would prefer not to agree a suspension or a termination right (of the cloud computing agreement or of single access to the services by its users) for the Provider in case of breach without providing the Adopter with the possibility of remedying such violation.

services or security for other customers. The Provider will be concerned that a very detailed and specific AUP is provided, aimed at prohibiting any possible conduct of the Adopter which may cause risks for the services and establishing all duties that the Adopter must comply with. If the Adopter breaches the AUP, the Provider shall be entitled to suspend and/or terminate the access of the users to the services or even the cloud computing agreement and remove any infringing content. Finally, in some cases, the Provider will also be keen to impose an obligation on the Adopter to cooperate with the Provider.	The Adopter would consider the termination of the entire cloud computing agreement for breach of some not serious obligations of the AUP by its users as a disproportionate remedy.
Position proposed by SLALOM	
It is important that the SLALOM AUP contains specific, non-generic language, setting out the exact obligations that the Adopter must fulfil. The AUP should also specify the rights of the Provider in circumstances where the AUP has been breached. This will help to establish a process for escalation: i) suspension of the access to the Services by the Users involved, ii) warning letter, iii) termination of the accesses of the Users involved in infringement of the AUP if no remedy has been taken[19]. In special cases, however, (e.g.: illegal activities or security risks), the suspension and removal of the Adopter Data may be performed by the Provider without any notice. We do not provide the termination of the entire CSA for infringement of the AUP by single Users of the Adopter because the possible conduct of single Users should not have such a strong and dangerous effect on the usage of the Services by the Adopter.	
Changes to the SLALOM proposed text after feedbacks	
1) We added, as an optional clause, the responsibility of the Adopter to back-up its data. It is worth stressing that this provision could have significant consequences in case of loss of data by the Provider, as the Provider can argue that the Adopter, in line with its obligations under the agreement, should be capable to recover the lost data by itself and/or that the Adopter cannot claim damages in relation to such loss because if the Adopter would have	

[19] Under German law, termination without notice is limited to narrow cases of "cause" (i.e. situations where continuing the contractual relationship is unreasonable due to the severity of the breach); in all other cases, typically, a prior notice and cure period is required. Accordingly, the Provider will always need to assess whether it is at risk of an unjust termination if it fails to establish the grounds for "cause". Similar provisions apply, mutatis mutandis, under Greek law, where provisions on contractual liability (Civil Code Articles 330, 334, 335, 336 and 382) combined with rules on tortuous liability and wrongful acts (Civil Code Articles 914-938) may be engaged against the terminating party, namely the cloud provider or the cloud adopter.

fulfilled its obligation to back-up its data, it would have not suffered any damages.
SLALOM proposed text
5.1 The Adopter shall use the Services in accordance with the Acceptable Use Policy under Attachment 3 to this Cloud Service Agreement. *5.2 The Adopter shall take all reasonable steps to ensure all the Users observe and fully comply with the terms of the Acceptable Use Policy when using the Services.* *5.3 If any User breaches any of the terms and conditions of the Acceptable Use Policy ("AUP"), the Provider shall have the right to suspend the User's access to Service such upon [two (2)] Working Days prior notice and to ask the User and/or the Adopter to remedy the breach within a reasonable timeframe. The Provider shall inform the Adopter of the above Users' breach as soon as it becomes aware of it. If the Users and/or the Adopter fail to remedy said breach within the applicable timeframe, the Provider shall have the right to (i) remove the Adopter Data infringing the AUP; and/or ii) immediately terminate the User's access to the Services without having to file a claim with the competent Court to that effect.* *5.4 If the Provider has reasonable evidence of i) possible serious risks to the System or Services provoked by the Adopter Data, or ii) fraudulent or illegal activities of the Adopter, the Provider is entitled to a) immediately suspend or terminate the accesses of the Users involved and b) to remove the relevant Adopter Data. If the circumstances in points a) and b) are proven to be false, the Adopter shall be indemnified for the damages suffered for the immediate suspension of the Services.* *5.5 The Adopter shall co-operate with the Provider to such extent as is reasonably practicable and necessary to enable the Provider to provide the Services.* *[OPTIONAL 5.6 The Adopter shall be responsible for maintaining, at its care and expenses, an appropriate and periodical back-up of the Adopter Data]*

Section 6: Charges

General description of the section
These provisions mainly have commercial implications. From a contractual perspective it is important to establish, as clearly as possible, i) what the charges will be or what criteria will apply in order to calculate the amounts due; ii) the scope of the underlying services and [any additional] activities and obligations which will need to be charged separately[20]. The consideration in cloud services can be calculated on usage (transactions, storage, users) measured on a monthly or periodic basis. In this case, the Provider is expected to provide the Adopter with a report of the use of the services to evidence the correct charges. The Italian law (Legislative Decree 231/2002, Article 5, para 1, in accordance with Directive

[20]Alessandro Musella, *Il Contratto di Outsourcing del Sistema Informativo*, Diritto dell'Informazione e dell'Informatica, 1998, pag. 868.

2000/35/EC ("on combating late payment in commercial transactions")) provides that the level of interest for late payment which the debtor is obliged to pay, shall be the sum of the interest rate applied by the European Central Bank to its most recent main refinancing operation carried out before the first calendar day of the half-year in question plus at least eight percentage points, unless otherwise specified in the contract.

Under French law, the payment terms and interest rates for late payments need to be specified[21]. Payment terms cannot exceed 60 days from the date of issuance of invoice (or 45 days from the end of the month where the invoice was issued) [22]. The standard/ default interest rate is the European Central Bank refinancing rate + 10%. The interest rate cannot be less than three times the then current legal interest rate. The agreement must also specify the amount of the fixed indemnity aimed at covering the costs incurred to recover the amounts owed by the Adopter (by default this fixed indemnity is € 40). Those provisions are deemed to be mandatory and will normally apply irrespective of the choice of law to the extent the Provider is established in France.

From a German legal perspective, cloud services will typically qualify as “rental services” and therefore, typically, need to define a recurrent remuneration scheme. Where upfront payments are made they are seen as covering the term of the lease. Furthermore, under German law, it would be rather common that the Provider modifies the Adopter’s statutory right to withhold or set-off payments for defective services, by limiting such right to cases where the counter-charge of the Adopter is undisputed or has been confirmed by finally binding court decision.

According to German law, If the Adopter fails to make timely payments then the Provider shall be entitled to charge interest on the overdue amount at a rate of 8% per annum, such percentage being the statutory entitlement under German law between merchants; 5 percentage points is the rule in all other relations.

Under Greek law 4152/2013 (which implemented EU Directive 2011/7 of 16 February 2011 “on combating late payment in commercial transactions”) where the debtor is a public authority the period of payment should not exceed 30 calendar days following the date of receipt by the debtor of the invoice or an equivalent request for payment or 30 days following the receipt if the goods or services.

The legislation in the UK allows the late interest rate up to 8% above base but most contracts include a lower negotiated amount.

Standard clauses used in the market

[21] Article L. 441-3 of the French Commercial Code.
[22] Article L. 441-6 I. of the French Commercial Code.

If the services are purchased on-line, the websites of the Provider provide the due consideration (or the parameters to calculate the due consideration) in the purchase process.

If the cloud computing agreement is executed off-line, the consideration (or the parameters to calculate the due consideration) is generally provided in an attachment of the agreement.

Some Providers provide the right to increase or add new fees for any existing services.

It is common providing interest for late payments.

In some cases, the cloud computing agreement establishes that the Provider may suspend the services upon notice in case the amounts due by the Adopter are not fully paid within the provided timeline.

Sometimes, the Providers establish a deadline for any claim of the Adopter in relation to due consideration. Once such deadline has expired, the Adopters may not raise any claim.

Provider's perspective	**Adopter's perspective**
From the Provider's perspective the types of underlying services (specifically certain activities or obligations) should be clarified. Such as, without limitation, possible changes to the services requested by the Adopter need an economical evaluation to ascertain possible changes of the due consideration (See paragraph 3 above).	The Adopter will be interested to ensure that the fees payable will include any and all activities and obligations under the cloud computing agreement, including where possible, all prospective changes of the services requested by the Adopter or any content provided by third-parties. The Adopter wants to ensure that the services and related activities are covered by the agreed charges and any activities that will be invoiced separately are clearly identified. Where charges are calculated based on usage, the Adopter will want to validate the usage figures and have a mechanism by which increased usage is authorised by an appropriate manager within the Adopter rather than by any user (who might not be aware of the cost implication).

Position proposed by SLALOM

The clause will be a standard payment clause for a service contract.

The consideration and most of the terms and conditions connected with payment shall be provided in an Attachment (see Attachment 4).

Most of the payment terms need to be included in the Attachment, taking into account the specifics of the relevant cloud Services and agreed payment model. We will mention however the Service Credits whose payment needs to be coordinated with the payment of Charges due.

Changes to the SLALOM proposed text after feedbacks
N/A
SLALOM proposed text
6.1 As consideration for the Services, and all connected performance and obligations of the Provider under this Cloud Service Agreement, the Adopter shall pay the Provider the Charges as detailed under Attachment 4, save for the provisions under Section 7 below. *6.2 The Adopter shall pay all undisputed invoices issued by the Provider in accordance with the requirements and the terms and conditions provided under Attachment 4.* *6.3 All Charges due to the Provider under this Cloud Service Agreement are exclusive of Sales Tax which where applicable shall be charged in addition thereto in accordance with the relevant regulations in force at the time of making the relevant taxable supply and shall be paid by the Adopter against receipt from the Provider of a valid Sales Tax invoice in respect thereof.* *6.4 If the Adopter fails to make payment in accordance with this Section 6 then the Provider shall be entitled to charge interest on the overdue amount at a rate of [to be inserted] % per year above the base rate of [to be inserted] from time to time in force from the date on which such amount fell due until payment, whether before or after judgment.* *6.5 Save as otherwise expressly provided in this Cloud Service Agreement, all Charges set out in Attachment 4 shall be deemed as fixed charges for the entire Term and fully inclusive of any and all activities necessary to supply the Services and all direct and indirect costs, taxes, charges or expenses relating to the Services.*

Section 7: Service credits

General description of the section
If the parties provide an SLA for the services, we need to understand the consequences of breaches of those service levels, otherwise, the SLA runs the risk of being ineffective[23]. Two main remedies in case of breach of the SLA are the accruing of services credits and the payment of penalties. The first consists of a reduction of the amount of charges to be paid; the second one relates to the amount to be paid by the Provider[24]. In German contractual practice, service credits are considered the same as contractual penalties.

[23] Kuan Hon, Christopher Millard & Ian Walden, *Negotiating Cloud Contracts: looking at clouds from both sides now*, Stanford Technology Law Review. Volume 16, Number 1 Fall 2012, pag. 97.

[24] Under Italian Civil Code, Article 1384, the "penalty clause" has the effect of limiting the compensation to the promised penalty, unless compensation was agreed on for additional damages. Under para 2 of Articles 1384 the penalty is due regardless of proof of damage.

Under English law, a penalty clause is unenforceable[25] while service credits or re-pricing mechanisms are permitted and used. As underlined by the DG Justice expert group (see Deliverable 4.1/5.1, Section 4.9.2), with reference to contracts with consumers, providing that the payment of the Service Credits is the only remedy of Adopters in case of breach of the SLA can be considered as an unfair clause under Directive 93/13/EEC. Accordingly, such clause could be considered as void. Under Italian Code of Consumers (Legislative Decree 206/2005, Article 33, para 2, sub-para b)) implementing above mentioned Directive 93/13/EEC, in case of contracts with consumers, the limitation of liability in the event of total or partial non-performance or inadequate performance by the seller or supplier of any of the contractual obligations, will be considered as an unfair term. Accordingly, in case of contract with consumers, providing that the payment of service credits is the exclusive remedy could be considered a void provision. Similar provisions are included within Greek consumer law 2251/1994, which implemented EU Directive 93/13/EEC. Furthermore, in accordance with the Italian law (Article 1341 of the Italian Civil Code), providing that the Service Credits will be the exclusive remedy for the breach by the Provider of the SLA may be considered as a burdensome clause (because it limits the liability of the Provider). If such burdensome clause is provided in a standard agreement drafted by one of the party, such clause (mentioned by its name and number) needs to be specifically approved in writing by the counterparty (even if it is not a consumer). If not specifically approved, the clause will be void. Such written approval may not be given by electronic means unless a digital signature (i.e.: kind of advanced electronic signature) is used, but only with a signature on the hardcopy of the agreement.
Standard clauses used in the market
The cloud computing agreements generally provide the criteria for calculating such service credits. Most of the agreements specify that the application of service credits is the exclusive remedy in case of breach of the SLA and that no other remedy or penalty is granted in favour of the Adopter.

[25] English law draws a distinction between 'penalty' clauses and 'liquidated damages'. Liquidated damages (that is, a fixed or pre-determined amount payable by a party on breach of contract) may be considered by the courts as recoverable. However as stated above, penalty clauses (i.e. clauses providing for a fixed amount which are designed to deter a party from breaking a promise rather than compensatory) may be construed as being unenforceable.
It should also be noted, that in order for a clause to be enforced as liquidated damages, the English courts will look at a number of factors. Traditionally, in order to establish whether the amount of damages required to be paid under the clause was not a penalty, the courts determined that a clause should provide for a 'genuine pre-estimate' of loss. In order to determine this, the courts construed that there must be a 'genuine commercial justification' for the clause, with the 'predominant purpose' being not to deter breach. More recent case law also considered to be 'extravagant' or 'unconscionable'. Recent case law also suggests that the courts will take social as well as commercial factors into account when determining whether a liquidated damages clause is not extravagant or unconscionable.
It is best to avoid the word “penalty” in English law contracts but, particularly in B2B contracts, the parties have a lot of flexibility to agree incentive or re-pricing mechanisms. Service credits are often expressly stated to be re-pricing mechanisms (rather than liquidated damages) to avoid any debate on this point.

In some cases, the Adopter, in order to have such service credits applied, needs to start a specific procedure providing the Provider with all information relating the service level violations.

Such data and information provided by the Adopter need then to be "validated" by the Provider. If they are not validated, no payment of service credits is due.

In some cases, the Providers provide a deadline for requesting the payment of service credits. After this deadline has expired, the service credit are not due.

Some Providers reserve the right to unilaterally change the service credits.

Some CSA provides a maximum amount of service credits which may be paid.

It is worth noting that in a few cases, the Providers do not provide the payment of service credit but establish that in case of breach of SLA, the remedy is the termination of the Agreement and the refund of any prepaid fees covering the remainder of the term the Agreement after the date of termination.

Provider's perspective	**Adopter's perspective**
The Provider may resist providing service credits in relation to possible violations of the SLA. Many Providers tend to provide the service credits as a sole and exclusive remedy, either for breach of service levels or, in some cases, all circumstances[26] so the Adopter has limited recourse for violation of other provisions of the agreement (e.g.: confidentiality obligations, infringement of third party rights). For the Provider it is quite important to clarify that once the service credits or penalties have been paid, no other amount or compensation shall be paid to the Adopter for possible damages the Adopter has suffered. From a French law perspective, the Provider will usually attempt to qualify the service credits as full and final compensation with respect to the breach of the service levels, exclusive of any additional remedy such as	The Adopter is very interested in claiming detailed service credits in case of violation of any SLAs and retaining the ability to claim damages for other material breaches of the agreement. This is generally considered as a good solution to prevent possible defaults by the Provider. The Adopter is interested in receiving reports concerning the identification of possible defaults by the Provider. In order to guarantee an immediate payment of the service credits (without being obliged to request them), an automatic set-off of the penalties with the due charges would be beneficial for the Adopter[27]. Furthermore, the Adopter is interested in providing that the service credits are not exhaustive of possible damages. Accordingly, if there are any further damages that can be proved, the Adopter will want to require the payment by the Provider of this additional amount.

[26] W. Kuan Hon, Christopher Millard & Ian Walden, *Negotiating Cloud Contracts: looking at clouds from both sides now, Stanford Technology Law Review. Volume 16*, Number 1 Fall 2012, pag. 98.

[27] Under the Italian Civil Code the set-off of the consideration (due by the Adopter) with the penalties (due by the Provider) can occur by means of Article 1241 and followings of Italian Civil Code.

damages or termination for breach.	Under the French contractual practice, the service credits being generally capped at a threshold between 5 and 15% of price of the monthly invoice, the Adopter will generally request that the service credits are not considered as a full and final compensation in respect of the failure to meet the service levels and to be able to seek remedies in addition to the trigger of the service credits. In the event a serious damage would be sustained by the Adopter, as a result, for instance, of the unavailability of the cloud services, the Adopter would then be entitled to seek damages on top or in lieu of the service credits. This would be possible only if the service credits do not qualify as "penalties" (*clause pénale*[28]) as such clauses are usually deemed to be exclusive of any other remedy in terms of damages. Under German law and in commercial practice, parties take a different view: the service credits are seen as "mini-penalties" each, which are essentially intended to incentivize proper performance. As a result, the Adopter's right to claim further damages is the default position. Moreover, a clause that potentially triggers recurrent penalty payments for similar breaches will need to be capped in the overall amount (such as by adding "… for such monthly period, provided however not to exceed an amount / percentage of xx% of the total contract value regardless of the number of breaches / triggering events."). Under Greek law, service credits are considered to provide a pre-specified financial remedy in the event of poor performance they are a form of liquidated damages. In order for the service credits to be enforceable by the customer, they must not exceed a reasonable pre-estimate of the customer's likely losses in the event of poor performance defined by market rules.
Position proposed by SLALOM	
A clause balancing the interests and positions of both the Provider and the Adopter should	

[28] A *clause pénale* is a clause whereby "*in order to guarantee the performance of an obligation, a person commits to do something in case of its failure to perform such an obligation*" (article 1221 of the French Civil Code).

provide service credits for most cases of breach of the SLA. In the SLALOM Agreement, we will provide two alternative clauses concerning the effects of payment of the Service Credits as this point is very often negotiated and discussed between the parties. In the first option we will provide that the payment of Service Credits and amount will be the exclusive remedy for the damages suffered for the breaches of specific SLA. In the second one, we will provide that the Adopter may claim for further damages within the limits provided under Section 12.2.2 of the Agreement (i.e.: liability cap). The criteria of calculation of the Service Criteria will be defined in the Attachment 2 of the Agreement which will be coordinated with this Section.
Changes to the SLALOM proposed text after feedbacks
N/A
SLALOM proposed text
7.1 If at any time the Provider fails to meet any Service Level Objectives, the Provider shall pay the Adopter the appropriate Service Credits in accordance with the following Sections 7.2 and 7.3. *7.2 The amount of any Service Credits payable under above Section 7.1, will be calculated in accordance with Attachment 2. Service Credits may be recovered by the Adopter as a credit against the next invoice which may subsequently be due for issue under this Agreement in accordance with above Section 6 or, if no such invoice is due, as a debt due by the Provider and payable within 30 (thirty) days after demand.* *7.3 The payment of the Service Credits under the above Section 7.1 states Provider's sole and entire obligation and liability, and Adopter's sole and exclusive right and remedy for any failure to meet the Service Levels under this Agreement.* *[ALTERNATIVE – 7.3 The payment of the Service Credits under the above Section 7.1 shall not limit the Adopter's right to claim compensation for any further damage and any other rights and remedies for the Provider's failure to meet any Service Level in accordance with the terms and conditions of Section 12.2.2 below.]*

Section 8: Intellectual property

General description of the section
This point raises many different legal and commercial issues. The clause concerns: i) the intellectual property rights of the Provider used to provide the services, ii) the intellectual property rights of the Adopter uploaded or used in receiving the services (and possible risks for the Provider in case of infringement of third parties' rights),

iii) the intellectual property rights of third parties providing applications on the platform of the Provider and possible connected development activities (i.e.: application management)[29].

Standard clauses used in the market

The cloud computing agreements normally provide that the Adopter retain all the intellectual property rights related to contents (database, software, texts, video, music, photographs, pictures, etc.) uploaded or created by the Adopter while using the services. The Provider, however, shall be entitled to use such contents to provide the services or, in some cases, also to comply with requests of competent authorities or bodies.

Some cloud computing agreements also provide a licence to the Provider for the content of the Adopter to improve the services or to guarantee their security.

On the other hand, many cloud computing agreements clarify that the Provider reserves all intellectual property rights relating to the services they provide in relation to their software or equipment.

Cloud computing agreements often provide that the Adopter has to guarantee or warrant that it has the right to upload, post, create the content.

In some cases, it is provided a kind of "licence to use the services" by the Provider to the Adopter.

The agreements often provide that, if the Provider believes that the services may infringe third party's intellectual property rights, the Provider may, at its discretion and expenses, (i) procure the right for the Adopter to continue using the services; (ii) modify the services to make them non-infringing (without reducing their functionality); or (iii) replace the services with a non-infringing, functionally equivalent alternative. Such remedies are provided as the only remedies in case of infringement of third party's intellectual property rights by the Provider.

Provider's perspective	**Adopter's perspective**
IPR of the Provider The Provider needs to state that all intellectual property rights in the components of the services shall vest in the Provider or are in its legitimate disposal. If the Provider creates any application or customisation (also required in relation to system integration activities) for the benefit of the Adopter, the Provider shall propose	*IPR of the Provider* Rather than being licensed the rights to use any applications modified or customised by the Provider, the Adopter is likely to require an assignment of the rights to use the software or materials. If an assignment is not possible, a second option is for the Adopter to seek a sole and exclusive license to use such materials and to prevent

[29] *Guidelines on Security and Privacy in Public Cloud Computing,* National Institute of Standards and Technology, U.S. Department of Commerce, 2011, pag.7; W. Kuan Hon, Christopher Millard & Ian Walden, *Negotiating Cloud Contracts: looking at clouds from both sides now, Stanford Technology Law Review. Volume 16*, Number 1 Fall 2012, pag. 126; European Commission, *Comparative Study On Cloud Computing Contracts, Final Report*, March 2015, pag. 41; Alessandro Musella, *Il Contratto di Outsourcing del Sistema Informativo*, Diritto dell'Informazione e dell'Informatica, 1998, pag. 877: Zincone, *Il Contratto di Outsourcing: natura, caratteristiche, effetti*, Rivista Dir. Autore 4/2002, pag. 401.

that all IPR in respect of such applications or customisations belongs to the Provider. The Provider will then grant licenses (exclusive or even not exclusive) on such software to the Adopter. *IPR of the Adopter* It would be in the Provider's interests to acquire licenses from the Adopter on the contents uploaded on the Provider servers[30]. The Provider would prefer to provide generic purposes relating to these licenses so that it can be entitled to use such content in its interests without many limits. On the other hand, the Provider will require an indemnity to cover it for possible third party infringements deriving from the content uploaded or created on the cloud platform by the Adopter. *IPR of third parties* With reference to software or materials provided by third parties upon request of the Adopter, the Provider should establish that it is not responsible for such software and materials and needs to be protected and indemnified in case of claims by third parties.	possible competitors to use the same software or contents. *IPR of the Adopter* It will be in the interest of the Adopter to authorize the Provider to use its content to the sole extent of providing the services excluding any other possible purpose. *IPR of third parties* It will not be in the interests of the Adopter to indemnify the Provider for possible claims from third parties both on the content uploaded by the Adopter and on the contents or software or application provided by third parties.
Position proposed by SLALOM	
This clause should distinguish amongst the competing interests of the Parties, with the aim of protecting all different entities involved. The parties will have to be informed of the rights of Third Parties which can be involved. The Parties need to provide a clear process in case Third Parties' rights are infringed, so that each party is aware of how to manage the matter, so as to limit the risk of conflict or the risk of termination.	
Changes to the SLALOM proposed text after feedbacks	
N/A	
SLALOM proposed text	

[30] European Commission's Expert Group Document, *Control and Use of Content*, pag. 1.

8.1 The Parties acknowledge that all Intellectual Property Rights belonging to a Party prior to the execution of this Agreement or created by the Parties regardless of the execution of this Agreement shall remain vested in that Party.

8.2 The Provider shall own, or shall have the legitimate right of disposal, in all Intellectual Property Rights in the Service, the Provider Content, the System and the Documentation and nothing in this Agreement shall operate so as to transfer or assign any such Intellectual Property Rights in the Service, Provider Content, the System and the Documentation to the Adopter. The Provider hereby grants to the Adopter a non-exclusive, worldwide, royalty free, non-transferable and non-sub licensable licence to allow the Adopter to access the System and use the Provider Content as well as any Provider's software which could be required to use the Services for the Term of this Agreement.

8.3 The Adopter shall own all Intellectual Property Rights in the Adopter Data and nothing in this Agreement shall operate so as to transfer or assign any such Intellectual Property Rights in such Content to the Provider, save for the following Section 8.4.

8.4 The Adopter hereby grants the Provider with a non-exclusive, worldwide, royalty free, non-transferable and non-sub licensable licence to use the Adopter Data solely and to the extent necessary to provide the Services, to the extent such access is required, without prejudice to the Intellectual Property Rights of the Adopter or any Third Party with respect to such Content.

8.5 In case the Provider installs on its System Third Party Content upon request of the Adopter, the Provider warrants and represents to own valid licenses on such Third Party Content and that it shall maintain the same licenses in full force for the all Term save otherwise agreed with the Adopter.

8.6 All Intellectual Property Rights related to Third Party Content installed on the System and used by the Adopter shall remain vested in such Third Party. The Adopter shall not be licensed or transferred with any right on such Third Party Content unless agreed by the Adopter with such Third Party.

8.7 The Adopter may upload in the System Third Party Content only upon prior authorisation of such Third Party.

Section 9: Term and termination

General description of the section
The duration of the agreement is mainly a commercial issue. However, having clear termination rights of both parties is both a commercial and legal issue. Therefore, the clause also concerns the right of termination of the agreement for the breaches by the other party of its obligations[31] and, if provided, the right of termination without cause on one or both the parties[32].

[31]Kuan Hon, Christopher Millard & Ian Walden, *Negotiating Cloud Contracts: looking at clouds from both sides now, Stanford Technology Law Review. Volume 16*, Number 1 Fall 2012, pag. 120; European Commission,

It is important to also consider the applicability of any provisions which survive the expiration or termination of the agreement (so called "post contractual obligations"). This point is included in the following Section 10 on "effect of expiration and termination".

In Germany, the terminating party must first notify of the breach and set a cure period; only afterwards a termination is permissible – unless terminating for "cause". In other words, termination will only occur following a separate and additional notice of termination after the cure period has elapsed fruitlessly.

It should be noted that under French law, in case one of the parties becomes subject to a bankruptcy and/or insolvency proceedings, a termination clause would not be valid since the receiver or liquidator appointed by Court has sole authority to decide whether the agreements entered into by the insolvent party should be discontinued[33].

Similarly, under German law solely the liquidator of the insolvent company has the authority to decide whether to honor the Agreement or not.

Italian Bankruptcy law (Royal Decree 267/1942, Article 72 n. 6; 186-bis, para 3) states that the agreement may not provide the termination of the agreement in case of bankruptcy or other insolvency procedures of one party.

Greek bankruptcy Code (law 4336/2015), which was adopted in line with the recent European Commission Recommendation C2014/1500 on a new approach to business failure and insolvency, provides that financial contracts of continued character can be terminated or amended, as a result of bankruptcy, following the performance of specific contractual insolvency clauses. Also, termination may still occur due to special provisions of the law (e.g. leasing contracts). This amendment seeks to preserve the value of the business of the debtor. Such provisions should be applicable on cloud contracts.

Standard clauses used in the market

The term of the agreement is generally provided in the subscriptions or the order form of the services purchased by the Adopter.

With reference to the right of termination, many cloud computing agreements provide the termination for convenience upon notice both for the Provider and the Adopter.

The cloud computing agreements also provide the right of termination for cause. By way of example, both parties shall have the right to terminate the agreement for material breach or

Comparative Study On Cloud Computing Contracts, Final Report, March 2015, pag. 51; Alessandro Musella, *Il Contratto di Outsourcing del Sistema Informativo*, Diritto dell'Informazione e dell'Informatica, 1998, pag. 869.

[32]With reference to contracts with consumers, according to Directive 93/13/EEC, Annex, Article 1, point f), the right of termination provided only for the Provider and not for the Adopter could be considered an unfair term which could be declared void.

[33] Paragraph I of Article L. 622-13 of the French Commercial Code provides that notwithstanding any contractual clause, any termination or cancellation of a current contract cannot result from the sole fact of receivership or liquidation proceedings' initiation (Commercial division of the Court of Cassation, January 14th, 2014 for receivership). This article applies to receivership and liquidation proceedings' initiation (Commercial division of the Court of Cassation, January 22th, 2002).

default of the other party which is not remedied by the other party in a certain period of time.

In some cases, the cloud computing agreements provide that the Provider may terminate the agreement if the contractual relationship with a third party providing software or other technologies expires. Then, the termination right in favour of the Provider is established also in case of security risks for the Provider or if the use of the services by the Adopter has become impractical or unfeasible for any legal or regulatory reason.

According to some cloud computing agreements, the termination right in favour of the Provider is provided also in case for inactivity of the Adopter which means that the Adopter is not using the services or that no bills are being issued by the Provider.

In some cases, the cloud computing agreements provide that either party may terminate the agreement if a change of control occurs to one party (e.g: a sale of the majority of shares carrying a right to vote in the company, or a change in the ownership of the legal power to direct the company).

Some cloud computing agreements provides that either party may terminate the agreement if the other party dissolves or otherwise ceases or threatens to cease to carry on its business; or goes bankrupt, an insolvency proceeding against such party has been opened or if it becomes unable to pay its debts, admits its inability to pay its debts.

Provider's perspective	**Adopter's perspective**
Term In certain circumstances, the Provider might want to specify in the agreement a longer term. This would need to be linked to a mechanism allowing for a charges review after a specific period of time to ensure that there is a mechanism to increase the fees (e.g. with a fee scale). Alternatively, the Provider might also prefer a more medium term agreement, whereby the term is re-negotiated prior to expiration along with fee scales. Another option would be to insert an automatic renewal provision with (if possible) a long notice term for preventing the renewal. Similarly, a charges mechanism linked to auto-renewal would also need to be included, allowing the Provider to increase the fees at regular intervals. *Termination* The Provider will be keen to include termination rights in its favour in case of a breach by the Adopter of its payment	*Term* The Adopter may be amenable to a longer term arrangement if the cloud services comprise the Adopter's core business activities (whereby a long and stable contractual relationship might be preferred). However, if the cloud services do not concern the core business activities of the Adopter (or in any case the migration activities are absent or not difficult), the Adopter might also be interested to negotiate short term agreements, allowing it to evaluate other possible Providers in the market. *Termination* The Adopter would prefer to have the right to terminate the agreement in case, the Provider has, for example: (i) breached a maximum threshold of services levels in the SLA; (ii) breached the intellectual property rights of any third parties;

obligation, or where there's a breach of third party rights, or if the Adopter has breached the law (e.g. by uploading content which is forbidden by law). Another option would be to insert an automatic renewal provision with (if possible) a long notice term for preventing the renewal. Similarly, a charges mechanism linked to auto-renewal would also need to be included, allowing the Provider to increase the fees at regular intervals. *Termination* The Provider will be keen to include termination rights in its favour in case of a breach, by the Adopter, of its payment obligation, or where there is a breach of third party rights, or if the Adopter has breached the law (e.g. by uploading content which is forbidden by law).	(iii) breached confidentiality or data protection obligations; (iv) breached the applicable law of the relevant country. Termination without cause provisions are also likely to be preferred by the Adopter.
Position proposed by SLALOM	
With reference to the Term, it would be opportune to provide a clause with a specific term to be agreed by the Parties which is not subject to automatic renewal so the parties can together evaluate and discuss the renewal of the agreement and the relevant conditions. The Parties will be entitled to terminate the agreement for breach only if the other Party does not remedy the breach upon receiving notice. We did not provide the right of the Party to immediately terminate the agreement for breach of any specific obligations by the other Party.	
Changes to the SLALOM proposed text after feedbacks	
1) We have added an optional clause providing the termination for convenience of either Party; 2) we have not provided any right of immediate termination of the CSA for breach of some provisions as we did not receive any feedbacks from the stakeholder requesting such type of provisions; 3) we added the right of termination of either Party where the other Party ceases to carry on business, is unable to pay its debts when they fall due, is declared bankrupt, or an order is made or a resolution passed for the winding up of that other Party or the appointment of an administrator, receiver, liquidator or manager of that other Party. Such clause is against the law in many jurisdictions. Accordingly, we provided that it is applicable to the extent permitted by the law; 4) we added the obligation to notify the termination with registered mail to avoid that such an important communication is given for instance via email among other less important communications.	

SLALOM proposed text
9.1 This Agreement shall commence on the Effective Date and shall continue in force for [x] years [or months] or until it is terminated in accordance with the Agreement. *9.2 Without prejudice to its other rights pursuant to law and this Agreement, if a Party is in material breach of one of its obligations under this Agreement, the other Party will have the right to terminate the Agreement by sending the other Party written notification via registered mail of any such breach, with the express invitation to remedy such breach within 30 (thirty) days of the date of receipt of the same notice. If such Party fails to remedy the material breach within such term, the Agreement shall be terminated.* *9.3 To the extent permitted by the applicable law, either Party may by written notice to the other Party immediately terminate this Agreement where the other Party ceases to carry on business, is unable to pay its debts when they fall due, is declared bankrupt, or an order is made or a resolution passed for the winding up of that other Party or the appointment of an administrator, receiver, liquidator or manager of that other Party.* *[OPTIONAL 9.4 Either Party may terminate without cause the Agreement upon [x] ([x]) days written notice to the other Party sent via registered mail].*

Section 10: Consequences of termination and expiration

General description of the section
It is very important to provide the obligations of the parties relating to the exit process. For the Adopter it is important to establish whether on expire or termination of the agreement, i) the data and content uploaded can be easily and quickly retrieved (also whether the format of the data is exportable and reversible) and ii) a new Provider shall be able to use such data and content, and iii) it can obtain an extension of the services until the new Provider is fully capable to provide the services[34]. Once the migration has concluded, it is important to ensure the deletion of the data and content of the Adopter, also to be compliant with data protection legislation and with possible confidentiality obligations provided by the parties. In particular, in case of processing of personal data, it is the Provider's duty to erase or otherwise destroy all personal data and certify that such personal data has been destroyed on its and its subcontractors' systems, or return any personal data in a structured and widely-used format with appropriate guarantees of portability. Indeed, as also noted by the ICO in the Guidance on the use of cloud computing, "*when data is deleted is it rarely removed entirely from the underlying storage media unless some additional steps are taken. In addition, a cloud Provider is likely to have multiple copies of data stored in multiple locations to provide a more reliable service. This may include back-up tapes or other media not directly*

[34]Kuan Hon, Christopher Millard & Ian Walden, *Negotiating Cloud Contracts: looking at clouds from both sides now*, Stanford Technology Law Review. Volume 16, Number 1 Fall 2012, pag. 122; European Commission, *Comparative Study On Cloud Computing Contracts, Final Report*, March 2015, pag. 52; European Commission's Expert Group Document, Switching – *Transfer and Deletion of Data After the End of the Relationship*, pag. 1; European Commission's Expert Group Document, Availability, pag. 1

connected to the cloud. Copies of personal data stored in a cloud service may also be stored in other forms such as index structures. ... The cloud customer must ensure that the cloud Provider can delete all copies of personal data within a timescale that is in line with their own deletion schedule". For a picture of some of the current positions from stakeholders and legal experts see Section 4.8.7.2 of the Deliverable 4.1 / 5.1.

For an analysis of the consequences related to the termination of the services please see also Section 4.6 of Deliverable 4.1/ 5.1

Standard clauses used in the market

As consequences of the termination or expiration, some cloud computing agreements specify that: (i) the Adopter will not be entitled to use the services; (ii) Adopter's rights under the agreement will cease; (iii) the Adopter shall be obligated to return or destroy the content provided by the Provider which are still in his/her possession; (iv) provisions concerning, among the others, indemnification obligations, the responsibility of the Adopter under the AUP, intellectual property rights, confidentiality obligations, shall survive such termination or expiration; (iv) all fees owed by Adopter to the Provider will be immediately due; (v) the governing law and jurisdiction provisions will continue to apply to the surviving terms.

In addition to the above, with reference to the content uploaded/created/published by the Adopter, most of the cloud computing agreements provide that the Provider shall not erase such content for a certain period of time (generally from 30 to 90 days) and that the Adopter shall be entitled to retrieve such content.

Some cloud computing agreements provide that the Adopter, in order to retrieve its data, has to pay a charge for the services performed by the Provider after the termination or expiration.

In some cases, the cloud computing agreements provide that upon termination for cause by the Adopter, the Provider will refund the Adopter any prepaid fees covering the remainder of the term of all order forms after the effective date of termination and if the agreement is terminated by the Provider for cause, the Adopter will pay any unpaid fees covering the remainder of the term of all order forms.

Provider's perspective	**Adopter's perspective**
The Provider, generally speaking, wants to bind the Adopter using technical standards which are not reversible or portable, or in general making the exit process more difficult. The Provider is interested in specifying that all activities connected with the exit process (migration of data, return of assets, or any other fulfilments) shall be paid by the Adopter (sometimes upon previous estimate by the Provider) and are not included in the charges already paid during the term of the agreement.	The Adopter would be concerned to ensure that: the data stored on the cloud is fully retrievable, it can easily migrate its content to other Providers in the marketplace, and have all confidential information and data returned or deleted. From a commercial perspective, the Adopter would also be interested in considering that the above activities are already included within the scope of the Services and all costs incurred in relation to them are paid during the term of the CSA or, otherwise, by ensuring that the Adopter receives the services upon a fair charge. The Adopter shall request that where the

	agreement has been terminated for convenience by the Provider or for cause by the Adopter (for breach of T&Cs by the Provider), all above-mentioned activities are provided free of charge by the Provider. The French Data Protection Regulation Authority (CNIL) has issued a set of recommendations with respect to cloud computing services which include standard clauses. One of these standard clauses[35] relates to destruction and restitution of data: *"At the expiry of the Contract or in the event of its early termination for any reason whatsoever, the Service Provider and his subcontractors if any shall return without delay to the Customer a copy of all the Data in the same format as that used by the Customer to communicate the Data to the Service Provider or failing this, in a structured and widely-used format.* *This restitution shall be ascertained by a report dated and signed by the Parties.* *Once the restitution has been carried out, the Service Provider shall destroy the copies of the Data held in his computer systems within a reasonable period and shall provide proof thereof to the Customer within a reasonable period following the signature of the restitution report"* Those standard clauses are now widely followed by French customers of cloud services.
Position proposed by SLALOM	
A clause trying to balance the interests of the Parties should state that, upon termination or expiration of the agreement, the Provider undertakes to return the Adopter Data to the Adopter or to transfer the Adopter Data to a new Provider (at Adopter's expenses). This is in line with the recommendations raised by some stakeholders (as well as the recent decision of the Tribunal de Grande Instance de Nanterre of 30 November 2012) as detailed in the Section 4.6 of the Deliverable 4.1/5.1. The Provider shall finally have the obligation to delete or destroy all Adopter Data from all systems which were used to provide the Services at the agreed time.	

[35] 2)b) of Appendix of Recommendations for companies that intend to subscribe to Cloud computing services (« *Recommandations pour les entreprises qui envisagent de souscrire à des services de Cloud computing* »), pag. 14

With reference to costs, we have distinguished between the different cases: the retrieval by the Adopter of Adopter Data shall be free of charge while the transfer of the Adopter Data to the Adopter or to any Third Party (including the new Provider) shall be at Adopter costs.

In line with the recommendations of experts groups mentioned under Section 4.6 of Deliverable 4.1/5.1, we have set forth that in the case of termination of the CSA due to breach by the Provider, the cost of transfer of the Adopter Data borne by the Adopter shall be reimbursed by the Provider.

The SLALOM proposal is in line with proposal for a directive on "Certain aspects concerning contracts for the supply of digital content" (COM(2015) 634 final) which in its Article 13, paragraph 2 (c), provides that in case of termination of the agreement:

"(c) the supplier shall provide the consumer with technical means to retrieve all content provided by the consumer and any other data produced or generated through the consumer's use of the digital content to the extent that data has been retained by the supplier. The consumer shall be entitled to retrieve the content free of charge, without significant inconvenience, in reasonable time and in a commonly used data format".

Above provision concerns the supply of digital content (including cloud computing services) to consumers. However, we deem that some of the principles included therein may be adopted also in business to business agreements.

We have set out a provision concerning the surviving of some clauses after the expiration or termination of the CSA.

Changes to the SLALOM proposed text after feedbacks

1) We provided a clear obligation of the Provider to not delete the existing Adopter Data until the Retrieval Period or the Transfer Period expires.

SLALOM proposed text

10.1 The Parties acknowledge and agree that in case of the expiration or termination for any cause of the Agreement:

10.1.1 the Provider shall not delete the then existing Adopter Data until the Retrieval Period or the Transfer Period under Sections 10.1.2 and 10.1.3 have expired;

10.1.2 upon request of the Adopter to be sent within [x] ([x]) days after the termination or the expiration date, the Adopter shall be entitled to retrieve the Adopter Data stored on the System in a structured and widely-used format, capable of ensuring portability of the Adopter Data, for a period of [x+n] (x+n) days after the expiration or termination date (hereinafter, "Retrieval Period");

10.1.3 upon request of the Adopter to be sent within [x] ([x]) days after the expiration or termination date, the Provider, at the Adopter's expense, shall transfer the Adopter Data in the format under Section 10.1.2 to the Adopter or to any Third Party provided by the Adopter within the agreed timing (hereinafter "Transfer Period"). If the Cloud Service Agreement has been terminated due to breach of the Provider, the Provider shall

reimburse the costs borne by the Adopter in relation to the above transfer of the Adopter Data;

10.1.4 once the Retrieval Period has expired, or upon completion of the Transfer Period, the Provider and its Subcontractors shall definitively destroy copies of, and erase, all Adopter Data stored in the System and all storage media and provides proof thereof to the Adopter within [x] ([x]) days following the expiration of the Retrieval Period or the Transfer Period, as applicable. The Adopter has the right to ask the deletion of the Adopter Data without any retrieval or transfer of the Adopter Data;

10.1.5 at the Provider's request, the Adopter will return or erase any of the Provider Content, data or software delivered or licensed to the Adopter for the purposes of providing the Services;

10.1.6 the Parties may agree any other possible activities or services connected with the expiration or termination of the Agreement upon mutual agreement of the Parties on the terms and conditions of such activities;

10.1.7 the rights, remedies, obligations or liabilities of either Party which have accrued up to the date of termination or expiry, will not be affected, including the right to claim damages in respect of any breach of the Cloud Service Agreement which existed at or before the date of termination or expiry;

10.1.8 any provisions of this Cloud Service Agreement which expressly, or by implication, are intended to come into or remain in force on or after termination or expiry of this Agreement, shall remain in full force and effect, including without limitation, Section 8 (Intellectual Property Rights), 10 (Consequences of Termination), 11 (Confidentiality Obligations), 12.2 and 12.3 (Warranties and Liabilities), 13 (Indemnification), 14 (Insurance Obligations); 17 (Data Protection); 19 (Notices – Party's Team Leaders); 20 (Governing Law); 21 (Disputes – Jurisdiction); and, 22 (Final Provisions).

Section 11: Confidentiality obligations

General description of the section
Many jurisdictions do not provide any form of statutory or legal obligation to keep confidential the information received by the other party during the execution of an agreement[36]. Confidential information does not generally include personal data (which is processed in accordance with data protection legislation and regulations (see Section 17 below). However, it is possible for confidential information to include personal data and vice versa. If the parties are interested in preventing the unauthorised disclosure of information relating, for

[36] Alessandro Musella, *Il Contratto di Outsourcing del Sistema Informativo*, Diritto dell'Informazione e dell'Informatica, 1998, pag. 883; Kuan Hon, Christopher Millard & Ian Walden, *Negotiating Cloud Contracts: looking at clouds from both sides now, Stanford Technology Law Review. Volume 16*, Number 1 Fall 2012, pag. 107; Giuseppe Prosperetti, *Diritto dell'Internet*, Cedam, edited by Giuseppe Cassano, Guido Scorza, Giuseppe Vaciagopag. 688; European Commission, *Comparative Study On Cloud Computing Contracts, Final Report*, March 2015, pag. 43.

instance, to their company, know-how, financial data, clients and customers, they will need to provide confidentiality obligations in their contract. If the Provider is not bound to such confidentiality obligations, it may be possible to argue that the Provider is entitled to disclose them to third parties.

Standard clauses used in the market

Some cloud computing agreements provide that only the Adopter is obligated to keep confidential the information that the Adopter has received using the services ("one-way" confidentiality agreement).

In other cases, the cloud computing agreements provide that both the parties reciprocally have such confidentiality obligations ("two-way" confidentiality agreement).

Such cloud computing agreements generally provide that the party receiving the confidential information will use the same degree of care that it uses to protect the confidentiality of its own confidential information of like kind but not less than reasonable care. Then the receiving party shall not disclose to any third party such information and shall not use any confidential information for any purpose outside the scope of the agreement.

It is generally provided that except as otherwise authorized by the disclosing party, the receiving party shall limit access to confidential information of the disclosing party to those who need that access for purposes consistent with the agreement and who have signed confidentiality agreements with the receiving party containing protections no less stringent than those provided by the agreement.

The confidentiality obligations shall normally provide also the cases in which the authorization of the disclosing party is not due such as, for instance, if such information has been received independently from a third party by the receiving party, if it becomes publicly available through no wrongful act or breach of the agreement by the receiving party; if it is independently developed by the receiving party, without referring to the disclosing party's confidential information; or if the information is required by law to be disclosed by the receiving party provided that the receiving party shall give to the disclosing party prompt notice of such request and the opportunity to oppose such disclosure or obtain a protective order at its request.

As said under the above "Term and Termination" Section, the confidentiality obligations normally survive the expiration or termination of the agreement.

Provider's perspective	**Adopter's perspective**
The Provider is interested in protecting any confidential information relating to the technologies behind its services which have been shared for the performance of the Services, or the information concerning its business which the Adopter could have received.	The Adopter will be concerned to ensure that all information uploaded by the Adopter or created or stored in any way in the cloud environment by the Adopter remains confidential. Such information should remain confidential also after the expiration or the termination (for any cause) of the agreement for a long period o time. It is important also for the Adopter to bind the Provider's current or future subcontractors

	involved with the provision of the Services.

Position proposed by SLALOM

Confidentiality obligations will be of interest to both Parties. Whereas the Adopter will be keen to ensure that all Adopter Data stored in the System is subject to a confidentiality undertaking, the Provider will be keen to protect certain data relating its own technologies (including source code), especially in circumstances where the Services have been subject to bespoke customisation, or where special technologies and know-how have been disclosed to the Adopter.

The confidentiality obligations should be reciprocal, and should define, in detail, who can access and use the data and for which purposes. The clause should also describe which information cannot be considered as confidential and that the confidentiality obligations shall survive the expiration or the possible termination or the agreement.

With reference to security measures, for the Provider we make reference to Attachment 6 while for the Adopter we provide some standard obligations.

Changes to the SLALOM proposed text after feedbacks

1) We reduced the term of the confidentiality obligations after the expiration or termination of the Cloud Service Agreement from 20 years to 6 years;

2) we added an exception in Section 11.9 to the above 6 years term of duration of the confidentiality obligations after the expiration or termination of the Agreement. Such term will not apply indeed in case of trade secrets. Trade secrets are protected under several jurisdictions as intellectual property rights without any time limit until they cease to be secret. If we provide a term of duration of confidentiality obligations on trade secrets, this could be interpreted as an authorization to disclose such trade secrets. Once disclosed, the trade secrets would lose the protection of the law.

SLALOM proposed text

11.1 During the Term, Confidential Information of the Disclosing Party may be learnt, developed or otherwise acquired by Receiving Party.

11.2 The Receiving Party will treat and keep all Confidential Information of the Disclosing Party as secret and confidential and will not, without the Disclosing Party's written consent, directly or indirectly communicate or disclose (whether in writing or orally or in any other manner) Confidential Information to any other person other than in accordance with the terms of this Agreement.

11.3 Section 11.2 shall not apply to the extent that the Receiving Party needs to disclose the Confidential Information of the Disclosing Party to any of its Group, or any Subcontractor in order to fulfil its obligations, exercise its rights under this Agreement or to receive the benefit of the Services, provided always that the Receiving Party shall ensure that every person to whom disclosure is made pursuant to this Section 11 uses such Confidential Information solely for such purposes, and complies with this Section 11 to the same extent as if it were a party to this Agreement.

11.4 Clause 11.2 shall not apply to any Confidential Information to the extent that:

11.4.1 such Confidential Information is in the public domain at the Effective Date, or at a later date comes into the public domain, where such Confidential Information has come into the public domain other than as a result of breach of this Agreement;

11.4.2 the Receiving Party can show that such Confidential Information was known to it before receipt pursuant to this Agreement, and had not previously been obtained or otherwise learnt under an obligation of confidence;

11.4.3 the Receiving Party obtains or has available to it, such Confidential Information from a source other than the Disclosing Party without breaching any obligation of confidence;

11.4.4 such Confidential Information is required by applicable law, or any competent regulatory authority [or recognised stock exchange]to be disclosed by the Receiving Party provided that the Receiving Party shall, where not prohibited, give to the Disclosing Party prompt notice of such request and the opportunity to oppose such disclosure or obtain a protective order at its request;

11.4.5 the Receiving Party can show such Confidential Information was independently developed or created by or on behalf of itself [or any member of its Group] otherwise than in connection with this Agreement, without the aid of any personnel who have or have had access to the Disclosing Party's Confidential Information; or

11.4.6 Information which the Disclosing Party confirms in writing is not required to be treated as Confidential Information.

11.5 If the Provider is the Receiving Party, the Receiving Party will use the Confidential Information of the other Party for the sole purpose of performing or complying with its obligations under this Agreement.

11.6 If the Provider is the Receiving Party, it agrees to implement and maintain the security measures under Attachment 6 to the Agreement.

11.7 If the Adopter is the Receiving Party, it agrees to implement and maintain to the Disclosing Party's reasonable satisfaction all reasonable security measures to safeguard the Disclosing Party's Confidential Information from unauthorised access, use or disclosure, and to ensure proper and secure storage of all Confidential Information and any copies thereof. Such measures shall be at least the same standard, whichever is the higher, as:

11.7.1 the Receiving Party keeps its own Confidential Information; or

11.7.2 the standard reasonably accepted as in line with the practices practiced in the same market.

The Receiving Party shall not make any copies or reproduce in any form any Confidential Information except for the purpose of disclosure as permitted in accordance with this Agreement.

11.8 Upon the termination or expiration of this Agreement or otherwise at the request of the Disclosing Party, the Receiving Party shall promptly return to the Disclosing Party all documents or materials in its control, custody or possession which contain, reflect, incorporate or are based on the Disclosing Party's Confidential Information and not retain

	any copies, extracts or other reproductions thereof or shall at the request of the Disclosing Party destroy all of the Disclosing Party's Confidential Information (erasing all Confidential Information from its computer systems or which is stored electronically) and certify in writing to the Disclosing Party that it has complied with the requirements of this Section.
11.9	*The obligations laid down in this Section 11 hereof shall remain the responsibility of each of the Parties, even after the termination or expiration of the Agreement on any ground, for the period of 6 (six) years from the said termination or expiration. With reference to any Confidential Information expressly identified as a trade secret, the confidentiality obligations shall extend indefinitely until a time when such information ceases to be a trade secret.*

Section 12: Warranties and liability

General description of the section
Contracts provide warranties for guaranteeing or acknowledging that the parties have certain titles or qualities or that the activities they will perform under the agreement have particular characteristics or features[37]. The liability of the Provider (and the possible limitation to such liability) is one of the main topics of cloud computing agreements[38]. Limitation of liability can be quantitative (a cap on the amount due) and qualitative (for some areas of contractual and extra-contractual responsibility)[39]. The limitations of liability in contracts with consumers can be considered as unfair clauses under Directive 93/13/EEC and therefore are considered to be void. Under French law, damages arising from gross negligence (*faute lourde*) or wilful misconduct (*dol*) cannot be limited[40]. Recent case law also set the rule that the liability caps and exclusions set forth in the agreement cannot result in depriving the other party from any actual remedy in the event of non-performance of a material obligation. The limitation of liability clause must reflect the allocation of risks and benefits under the agreement and not be "derisory" [41].Furthermore, according to French law, it is not possible to limit or exclude liability in consumer contracts[42]. From a German legal perspective, the above considerations can only work if the terms are negotiated and agreed individually – which in many instances is the rare exception. When using general terms of contract, German courts are rather strict in regard to limitations of liability even

[37]Kuan Hon, Christopher Millard & Ian Walden, *Negotiating Cloud Contracts: looking at clouds from both sides now*, Stanford Technology Law Review. Volume 16, Number 1 Fall 2012, pag. 94.
[38]European Commission's Expert Group Document, Liability For non-performance including remedies, page 1; Dimosthenis Kyriazis, *Cloud Computing Service Levels Agreements, Exploitation of Service Level Results*, pag. 34; W. Kuan Hon, Christopher Millard & Ian Walden, *Negotiating Cloud Contracts: looking at clouds from both sides now, Stanford Technology Law Review. Volume 16*, Number 1 Fall 2012, pag. 94.
[39] European Commission, *Comparative Study On Cloud Computing Contracts, Final Report*, March 2015, pag. 46.
[40] icle 1150 of French Civil Code.
[41] Commercial division of the Court of Cassation, June 29th, 2010, "*Faurecia*".
[42] Paragraph 6 of Article R. 132-1 of the French Consumer Code.

in B2B contracts. Limitations on wilful misconduct and gross negligence in regard to bodily harm as well as cases of mandatory liability (product liability etc.) will be unenforceable, as well as providing exclusions and caps that go further than the "typically foreseeable damage" in case of a breach of a material contractual obligation (so called "cardinal obligation") by way of simple or slight negligence. Accordingly, liability clauses entirely excluding or capping liability for indirect damages are potentially unenforceable, too.

Under Greek consumer law (law 2251/1994 Article 6) any service provider is liable for defective products or services. Liability exclusions are very limited. The service provider may be prosecuted in case of concurrence of contractual and tortuous liability when the act or omission that resulted to the damage, injury or death constitutes a violation of a contractual obligation and at the same is deemed as a “wrongful” (tortuous) act or omission. Depending on the business context, there are special pieces of legislation which apply on top or are complementary to the general provisions of the Civil code.

Under English law, the parties cannot exclude liability for fraudulent misrepresentation or death/personal injury caused by negligence. However, if carefully addressed, it is possible to exclude liability for wilful default and there is no defined concept of “gross negligence”.

The Italian law (Article 1229 of Italian Civil Code) provides that the parties cannot limit or exclude liability in case of wilful misconduct and in case of gross negligence. Furthermore, according to Article 33, para 2 of the Code od Consumers (Legislative Decree 206/2005) implementing above mentioned Directive 93/13, in case of contract with consumers, the limitation of liability in the event of total or partial non-performance or inadequate performance by the seller or supplier of any of the contractual obligations, will be considered as void (even if specifically negotiated).

Standard clauses used in the market

It is worth noting that some cloud computing agreements provide that the services shall be provided "as is" without any particular representation or warranties. The Provider disclaims all implied warranties, including any implied warranty of merchantability, fitness for a particular purpose or non-infringement, to the maximum extent permitted by applicable law.

In some cases, the agreement states that the Provider does not warrant that the operation of the software or the services will be error-free or will be performed without interruption.

In some other cases, the Provider warrants that it will perform the services in accordance with the SLA and that no other warranty is given.

Some cloud computing agreements provide that the Provider will be not responsible if the Adopters cannot use the services in consequences of total or partial unscheduled downtime of the services; termination or suspension of the agreement; Provider’s interruption of any or all of the services; and for any kind of expenses the Adopter has to borne for the failure of the Provider to provide the services.

In some cases, the cloud computing agreements establish that the Provider will not be responsible for unauthorized access to the Adopter’s content or in case of loss, deletion or alteration of the content or other data uploaded by the Adopter. In other cases, cloud computing agreements establish that the Adopter is obligated to copy or back-up its data or content.

Most of the cloud computing agreements specify that some kind of damages are excluded such as direct, indirect, incidental, special or consequential damages (as for instance, loss of profits or goodwill) or punitive damages.

It is common providing that the maximum liability of the Provider is limited to the consideration paid by the Adopter in the 12 months prior to the event giving rise to liability.

Sometimes, the above cap on liability is excluded for the breach of some kind of obligations such as confidentiality obligations, violations of a party's intellectual property rights by the other party, or indemnification obligations.

Provider's perspective	**Adopter's perspective**
Warranties For commercial parties, the Provider will look to receive a warranty from the Adopter that the representatives executing the cloud computing agreement on behalf of the Adopter have the power to validly bind the company. *Liability* The Provider will require very strict limits on its liabilities. This is likely to result in extensive liability caps on the amounts the Adopter may seek to claim in damages and a number of exclusions of liability (including losses resulting from data use and data loss). The Provider may also try to propose that the payment of service credits is exhaustive of possible damages in relation to the relating services.	*Warranties* The Adopter will want to ensure that it has received extensive warranties confirming that the Provider will, for example, perform the services properly etc. (i.e.: structures, equipment). *Liability* The Adopter would be interested in providing that the Provider is responsible without limitations for executing the cloud computing agreements [43] (save for possible limitations and criteria of responsibility provided by the law). If it is not possible to provide the above and the liability of the Provider is limited within a certain amount, the Adopter shall try to exclude some areas from the limitation of liability. This is a sensitive choice since possible breaches of confidentiality or intellectual property of third parties, as well as possible violations of the applicable legislation (e.g.: anti-bribery, data protection) cannot be considered connected with the "value of the contract" (i.e.: the consideration to be paid). Such kind of violations, indeed, can be considered as not directly related to the performance of the services so deserving to be considered as not included in "normal liability

[43] Such as for instance Article 1223 of Italian Civil Code providing that "*The measure of damages arising from non-performance or delay shall include the loss sustained by the creditor and the lost profits insofar as they are a direct and immediate consequence of the non-performance or delay*"). Moreover, Article 1225 of Italian Civil Code provides that "If the non-performance or delay is not caused by the fraud or malice of the debtor, compensation is limited to the damages that could have been foreseen at the time the obligations arose". With reference to exoneration of liability clauses, Article 1229 c.c. provides that "Any agreement which, in advance, excludes or limits the liability of the debtor for fraud, malice or gross negligence is void".

	criteria" of the contract.

Position proposed by SLALOM

The SLALOM CSA could provide a cap to be determined by the parties taking into account the value of the contract and the possible damages they may suffer.

Such damages suffered by the Adopter can be higher if the cloud services relate, for instance, to activities which are the core business of the companies and can be lower if the Services relate to activities which are not fundamentally important to the Adopter, but this will not always be the case.

The damages connected with some kind of breaches such as breach of the confidentiality obligations and breach of intellectual property rights of Third-Parties shall not be limited under the above cap (see Deliverable 4.1/5.1, Section 4.9.1).

It is advisable also to remember that certain legal claims cannot be excluded: such, depending on the applicable law, as willful misconduct, fraud, gross negligence, personal injury, or damage to health caused with intent or negligence[44].

As the suggested limitation to liability is reciprocal, it will apply also in case of possible breach of the AUP by the Adopter.

Changes to the SLALOM proposed text after feedbacks

1) In Section 12.1.1.4, we changed the "best effort" by the Provider to ensure that the Services, the Provider Content, the System and the relevant software are free from all viruses into a "reasonable effort". Accordingly, the obligations of the Provider in this respect will be less strong and engaging and more close to the standards of the sector (most of the agreements used in the market indeed does not provide any obligations of this kind);

2) we added the breach of Clause 17 (Data Protection) as one of the cases in which the limitation to liability of the Parties does not apply.

SLALOM proposed text

12.1 Warranties

12.1.1 The Provider represents and warrants that:

12.1.1.1 the Services will be performed with reasonable skill and care in a timely and professional manner using appropriately qualified and experienced personnel and in accordance with good industry practice;

12.1.1.2 the Services will be performed in accordance with the security requirements provided under Attachment 6 to this Agreement and in accordance with all

[44]European Commission, *Comparative Study On Cloud Computing Contracts, Final Report,* March 2015, pag. 46.

applicable laws and regulation on security in the communications and in the provisions of information society services;

12.1.1.3 it owns or has obtained valid licences of all Third Party Intellectual Property Rights relating Third Party Content or which are necessary for the performance of any of its obligations hereunder;

12.1.1.4 by performing the Services under this Agreement, the Provider will not infringe any Intellectual Property Rights of any Third Party;

12.1.1.5 it shall use its reasonable efforts to ensure that the Services, the Provider Content, the System and the relevant software are free from all viruses and other contaminants including any codes or instruction that may be used to access, modify, delete or damage any data files, or other computer programs used by the Adopter from time to time, and that for this purpose, the Provider warrants and represents that it shall use the most comprehensive and up to date available virus checker;

12.1.1.6 it has the full capacity and authority and all necessary licenses, permits and consents from Third-Parties to enable it to enter into this Agreement and perform all of the Providers' obligations hereunder;

12.1.1.7 this Agreement is executed by a duly authorised representative of the Provider.

12.1.2 The Adopter represents and warrants that

12.1.2.1 It owns or has obtained valid licences of all Intellectual Property Rights in relation to the Adopter Data uploaded on the System including possible software of Third Party installed, uploaded or developed on the System;

12.1.2.2 It has the full capacity and authority and all necessary licenses, permits and consents from Third-Parties to enable it to enter into this Agreement and perform all of the Provider's obligations hereunder;

12.1.2.3 this Agreement is executed by a duly authorised representative of the Adopter.

12.2 Liability

12.2.1 Neither Party limits or excludes its liability:

a) for acts or omission due to wilful misconduct of either party;
b) in respect of any deceit, theft, fraud or fraudulent misrepresentation by its employees, consultants or Subcontractors;
c) for death or personal injury caused by its negligence or that of its employees, consultants or subcontractors, as applicable;
d) under Section 8 (Intellectual Property Rights);
e) for breach of Clause 11 (Confidentiality);
f) for breach of Clause 17 (Data Protection);

g) to the extent that such limitation or exclusion is not permitted by law.

12.2.2 Subject to Section 12.2.1, the maximum aggregate liability of either Party arising under or in connection with this Agreement (whether in tort (including for negligence or breach of statutory duty), contract, misrepresentation (whether innocent or negligent), restitution or otherwise) shall be limited to the amount of [TO BE DETERMINED]. The limitation of liability under this Section 12.2.2 shall not apply in the event the Adopter is a consumer (i.e.: natural person acting for purposes which are outside his trade, business, craft or profession).

12.2.3 Service Credits shall be taken into account when assessing whether the liability caps set out in above Section 12.2.2 have been met or exceeded.

[ALTERNATIVE - 12.2.3 Service Credits shall not be taken into account when assessing whether the liability caps set out in above Section 12.2.2 have been met or exceeded].

Section 13: Indemnification

General description of the section	
The indemnification section provides details of the indemnification obligations of the parties[45].	
Standard clauses used in the market	
Some cloud computing agreements establish that the Provider will defend the Adopter against any claim brought against the Adopter by a third party alleging that the use of a service infringes such third party's intellectual property rights. In this case, the Provider will indemnify the Adopter from any damages and costs awarded against the Adopter as a result of above claims. Cloud computing agreements often provide some conditions to the above indemnification obligation against third party claims such as that the Adopter is required to give the Provider (a) (a) written notice of the claim, (b) sole control of the defence and (c) all reasonable assistance, at Provider's expense. With reference to the indemnification obligations of the Adopter, it is often provided that the Adopter will defend and indemnify the Provider from any claims and expenses arising out of or relating to any third party claim concerning the Adopter's use of the services or the Adopter's breach of the agreement or violation of applicable law or arising out of uploaded/created content; or violation of the AUP by the Adopter. For further information on indemnification on intellectual property rights see paragraph 8 above.	
Provider's perspective	**Adopter's perspective**
The Provider will want to ensure that the	The Adopter will want to ensure that the Provider

[45]Kuan Hon, Christopher Millard & Ian Walden, *Negotiating Cloud Contracts: looking at clouds from both sides now, Stanford Technology Law Review. Volume 16*, Number 1 Fall 2012, page 94.

Adopter safeguards and indemnifies the Provider for any possible damages which could be incurred as a result of the Adopter uploading content on to the Provider's server which breaches the terms and conditions of the AUP. Such indemnification shall include, without limitation, possible breaches of intellectual property rights, data protection rights of third parties, or confidentiality obligations.	pays all damages the Adopter has incurred as a consequence of a default of the Provider supplying services, or in case of a breach of any other important obligations of the contract or in the case of claims by third parties. The Adopter will also be concerned to ensure that the payment of service credits excludes all possible damages that the Adopter has suffered as a result of a default of the Provider.

Position proposed by SLALOM

The indemnification clause should reflect the criteria and principles provided under the liability clause. The indemnification clause will mainly focus on the infringement of IP obligations and of the AUP by the Users.

With reference to infringement of IP obligations by the Provider, the clause provides a process with several different options to avoid the infringement. The Provider shall at its discretion decide the best option. In any case, the Provider will have to guarantee the continuity of the business of the Adopter.

The indemnity provided by the Adopter will concern both possible infringement of Third Party Intellectual Property Rights and breach of the AUP by the Users.

With reference to this last indemnity the limitation of liability under Section 12.2.2 shall apply.

Changes to the SLALOM proposed text after feedbacks

N/A

SLALOM proposed text

13.1 The Provider shall indemnify on demand the Adopter and the Adopter's assignees, directors, partners, officers, employees and agents against on demand against any and all losses, claims, damages, costs, expenses (including without limitation legal fees) and liabilities which the Adopter may sustain or incur or which may be brought or established against it by any Third Party in respect of any ascertained breach of the warranties set out in Sections 8.2, 8.5, 12.1.1.2, 12.1.1.3 of the Cloud Service Agreement ("IPR Claim").

13.2 The Adopter agrees:

a) it shall promptly, upon becoming aware of any IPR Claim, notify the Provider and provide to the Provider reasonable assistance, at the Provider's expense, which the Provider may reasonably request in connection with the defence of any such IPR Claim; and

b) it shall not make any admission as to liability or compromise or agree to any settlement or any IPR Claim without the prior written consent of the Provider which consent shall not be unreasonably withheld or delayed.

13.3 If any IPR Claim is made, the Provider shall at its own expense and sole option either: *13.3.1 obtain for the Adopter the right to continue using the Services, the Provider Content, and the Third Party Content in the manner permitted under this Agreement; or* *13.3.2 modify or replace the infringing part of the Services, the Provider Content, or the Third Party Content so as to avoid the infringement or alleged infringement, without prejudice to the representations and warranties in Section 13.1.* *13.4 The Adopter shall defend, indemnify and hold harmless the Provider and the Provider's assignees, directors, partners, officers, employees and agents on demand from and against any and all losses, claims, damages, costs, expenses (including without limitation legal fees) and liabilities which the Adopter may sustain or incur or which may brought or established against it by any Third Party in respect of any ascertained breach of the warranties set out in Sections 5.2, 8.3, 12.1.2.1.* *13.5 The Parties shall comply with the indemnification obligations provided by the present Section 13 in accordance with the terms and conditions provided under above Section 12.2.*

Section 14: Insurance obligations

General description of the section	
The Adopter will want to insure against the possibility of the Provider being unable to pay damages incurred as a result of a breach of contract (e.g. being unable to provide the services). As a result, the Adopter will want to ensure that the Provider has in place an insurance policy covering all possible damages that the Adopter can receive as a result of the non-performance of the services by the Provider or, in general, by executing its obligations under the cloud computing agreement[46].	
Standard clauses used in the market	
These kinds of obligations are generally not provided in the standard agreements executed with main public cloud Providers. Where such insurance policies are provided, the relevant clause may sometimes establish the overall amount that the insurance may pay (for each event and in aggregate). With reference to cloud computing agreements which are specifically negotiated by the parties, the insurance policy is sometimes attached to the agreement.	
Provider's perspective	**Adopter's perspective**

[46]European Commission's Expert Group Document, Liability For non-performance including remedies, page 1.

The Provider will usually insist on having a generic provision on insurance obligations which reflects the insurance policies which the Provider will already have in place.	The Adopter will usually require a provision obliging the provider to implement appropriate insurance which covers all possible damages which the Adopter could incur in relation to the performance (or lack of performance) of the services. The Adopter will request to provide in the limitations on liability (in aggregate and for single event) the amount that can be paid by the insurance company. Such amount has to be proportionate to the effective damages that the Adopter has actually suffered in case of non-performance by the Provider of its obligations. Since the damage arising from the performance of the cloud services could be detected after the termination or expiration of the cloud computing agreement, the Adopter will request that the insurance obligations shall survive the termination/expiration of the cloud computing agreement.
Position proposed by SLALOM	
The clause on insurance obligations under the CSA will provide that the Provider guarantees that it will have adequate insurance in place to cover it against damages resulting from a breach of the CSA by the Provider. The maximum amount payable by the insurance company will be decided by the Parties but will effectively be the limits of the provider's insurance policies. It cannot be the same amount provided under Section 12.2.2 as cap to liabilities of the parties, because some areas of liability (such as IP or confidentiality) are not subject to such limitation. The Provider should also agree that the insurance policy shall be in place for at least two years after the expiration/termination of the Agreement. The insurance policy will not be attached to the Agreement.	
Changes to the SLALOM proposed text after feedbacks	
N/A	
SLALOM proposed text	
14.1 The Provider shall maintain, during the Term of this Agreement [and for a period of at least 2 (two) years after the expiration or termination of the Agreement], appropriate insurance policies in relation to any liability connected with the execution of this Agreement with a reputable insurance company in respect of the Provider's performance of the Services, providing for the payment of a sum up to [TO BE DEFINED] for any claim or series of claims arising out of a single event occurring during such period.	

Section 15: Suspension of services

General description of the section
Under some legal systems, each party (unless such right is excluded by the CSA), can suspend the performance of its obligations if the other party does not perform its obligations under the CSA[47][48]. For instance, in case of non-payment by the Adopter (or in case of a breach of the AUP), the Provider could be entitled to suspend the services[49]. On the other hand, the Adopter could be entitled to suspend the payment if the Provider does not fulfil its obligations under the CSA. Other than in cases where the other party has defaulted and, with particular reference to cloud services, the Provider may also wish to suspend the services for technical reasons (i.e.: for maintenance of the services). In accordance with Italian law (Article 1341 of the Italian Civil Code), providing that the Provider may suspend the services may be considered as a burdensome clause. If such burdensome clause is provided in a standard agreement drafted by one of the party, such clause (mentioned by its name and number) needs to be specifically approved in writing by the counterparty (even if it is not a consumer). If not specifically approved, the clause will be void. Such written approval may not be given by electronic means unless a digital signature (i.e.: kind of advanced electronic signature) is used, but only with a signature on the hardcopy of the agreement. Similarly, under Greek law, to be valid, unilateral contractual amendments need to be approved by the other party. Otherwise such clauses provide a reason for early contract termination and request for damages by the other party.
Standard clauses used in the market
Cloud computing agreements often establish that the Provider may suspend the provision of services in case for instance of violation of the AUP by the Adopter, in case of risks to security posed by the Adopter, or in case of violation of rights of third party. Furthermore, according to some cloud computing agreements, the Provider will be entitled to suspend the services in case of breach by the Adopter or in case of its bankruptcy, insolvency proceedings, dissolution or similar proceeding. Depending on the cause of the suspension, in some case, the suspension is given upon notice

[47]See Article 1460 of Italian Civil Code providing that "*In contracts providing for mutual counter-performance, each party can refuse to perform his obligations if the other party does not perform or offer to perform his own at the same time, unless different times for performances have been established by the parties or appear from the nature of the contract. However, performance cannot be rejected if, considering the circumstances, such rejection is contrary to good faith*". Kuan Hon, Christopher Millard & Ian Walden, *Negotiating Cloud Contracts: looking at clouds from both sides now, Stanford Technology Law Review. Volume 16*, Number 1 Fall 2012, pag. 124.

[48] Under Uk laws there are no such legislative rights.

[49]W. Kuan Hon, Christopher Millard & Ian Walden, *Negotiating Cloud Contracts: looking at clouds from both sides now, Stanford Technology Law Review. Volume 16*, Number 1 Fall 2012, pag. 124.

and in some case (as in case of security threats) is immediate.

Some cloud computing agreements provide that, during the suspension, the customer remains responsible for the payment of all fees and charges.

It also provided that the service credits are not due during the suspension period.

The right of suspension is in addition to the right of termination of the Provider which is often triggered by the same causes and circumstances triggering the suspension.

Some cloud computing agreements provide the right of suspension of the service in case of failure of payment of the charges due by the Adopter.

Provider's perspective	**Adopter's perspective**
The Provider needs to establish that in some cases (for instance in case of maintenance/update of its servers) it has the right to suspend the services.	The Adopter does not normally require the suspension of the services (especially if the services are provided on a volume basis, based on the consumption of services used). However, where suspension rights are necessary, the Adopter will want to ensure that i) the period of suspension is short; and ii) date of suspension is agreed beforehand. The Adopter will also want to ensure that, after the end of the suspension period, the Provider immediately and fully restores the services.

SLALOM proposed text

The SLALOM proposed text only takes into consideration suspension rights as a result of technical reasons. The suspension for non-fulfilment of obligations by the Adopter is provided under above Sections 5.3 and 5.4. We do not provide the right of suspension of payment for the Adopter.

A clause balancing the interests of both the Parties should also provide for the possibility of the Provider suspending the Services if this is needed to update or maintain its servers or equipment. Such suspension should occur upon a fair notice (i.e.: not less than 10 working days). The Provider should duly communicate the timing and duration of suspension and shall guarantee (in the form of an SLA) the timing for completely restoring the Services.

In case the Adopter (due to serious reasons related to its business operating) communicates that the suspension could cause serious damages to its activities, the Parties shall discuss possible postponement of the suspension which cannot be unreasonably refused by the Provider.

In this respect, we must consider that the postponement should be not feasible in case of multi-tenancy Systems. For this reason, we have provided the words ""unless such postponement is not feasible due for technical reasons".

Changes to the SLALOM proposed text after feedbacks
1) We slightly changed the Section 15.2 to have a clearer wording of the rights and obligations of the parties.
SLALOM proposed text
15.1 The Provider may suspend the provision of the Services, by giving the Adopter no less than 10 (ten) Working Days' notice, in circumstances where it is necessary for the Provider to update or maintain the System. The Provider shall, in its notice, inform the Adopter of the timing, the duration and the reasons for the proposed suspension. *15.2 The Adopter shall be entitled to request in writing a postponement of the suspension. The Provider shall not unreasonably deny its consent to the above request of the Adopter. Without limitations, the Provider may reject the postponement if it is not feasible for technical reasons.*

Section 16: Subcontracting

General description of the section
This clause provides the rules relating to the subcontracting of all or part of the services from the Provider to a third party[50]. The parties can provide that the subcontracting by the Provider should be previously approved by the Adopter or instead that the Provider can subcontract without receiving authorisation. In accordance with Italian Civil Code, the subcontracting has to be authorized by the Adopter (Article 1656). The parties however may derogate to this provision of law, agreeing that the Provider may appoint subcontractors without the authorization of the Adopter. If personal data is processed by the Adopter using the services, under some jurisdictions (among the others, Italy, UK and Greece), the Adopter may also be required to keep control of the circulation of personal data and of the identity of all those who process personal data as (sub) processors, including subcontractors,[51] and this clause must explicitly refer to the data protection obligations which are normally included in an attachment to the Agreement (such as the Attachment 5 of the SLALOM CSA). Subcontracting is optional; however, if the Provider ever engages in any subcontracting, the agreement should include this section and the relevant corresponding section under Attachment 5 is essential to seek compliance with most of the applicable data protection legislations. For a picture of some of the current positions from stakeholders and legal experts see Section

[50] Article 1656 of Italian Civil Code provides that the contracted party may subcontract the activities to be performed under the agreement only upon approval of the customer; European Commission, *Comparative Study On Cloud Computing Contracts, Final Report*, March 2015, pag. 49.
[51] European Commission's Expert Group Document, *Subcontracting*, March 25, 2014.

4.7 of the Deliverable 4.1 /5.1. According to the results of the SLALOM Questionnaires circulated by SLALOM during the Cloud Expo Europe on March 2015, managing subcontracting and ensuring standardization of the obligations in this context is one of the major issues (see Section 3.4.4 of Deliverable D.4.1 / 5.1).

Standard clauses used in the market

Most Providers (especially main public cloud Providers) do not provide any clause in relation to subcontracting.

Some cloud computing agreements set out that the Provider may hire subcontractors to provide services whilst the provider remains responsible for the correct performance of its obligations under the agreement. In this case, the Adopter agrees to transfer its uploaded/created content to subcontractors as described in the agreement.

With reference to data protection issues, any above subcontractors will be permitted to obtain customer uploaded/created content only to deliver the services the Provider has retained them to provide and will be prohibited from using customer uploaded/created content for any other purpose.

Provider's perspective	**Adopter's perspective**
The Provider would be concerned to retain a right to subcontract without receiving any authorisation from the Adopter. As a second option, the Provider could request that it has full discretion as to whether to subcontract the agreement, provided that it informs the Adopter, identifying the third party and the activity subcontracted.	In some jurisdictions[52], data protection legislation may require that the CSA clearly (i) identifies who the third party subcontractors are and (ii) provides the Adopter with the right to deny its consent to such subcontract for any reason. The Adopter will request that all applicable obligations of the agreement also apply to the third party (e.g. confidentially obligations, fulfilment of the SLA, and data protection obligations) and that only the Provider shall remain responsible for indemnifying the Adopter for any breach of the agreement caused, as a result, of the third party's actions or omissions. Finally, it will be important for the Adopter that the Provider remains the only point of contact during the term of the agreement, unless the Adopter itself requests to contact directly the subcontracted party.

[52] By way of example, Spanish Supreme Court (ruling dated 15 July 2010) considered that it is data processor's duty to inform in advance the data controller of details of subcontractors as the provider, as data processor, cannot take autonomously decisions about the processing (the same principles applies also in Italy). In the same ruling it was considered that the Adopter should also be informed of the country/-ies where its services are based and, in case of subcontracting and of its disagreement, the Adopter is entitled to terminate the agreement or refuse that sub-contractors are appointed.

Position proposed by SLALOM
The Provider, under this clause, will have the right to subcontract the Services, provided that it keeps the Adopter informed as to the identity of the third parties who will be performing the sub-contracted services. This position should meet the concerns of the stakeholders provided in the SLALOM Questionnaire about the importance of knowing which Third-Parties may be involved in the services (see Deliverable 4.1/5.1, Section 4.7). If the Services offered under the CSA include personal data, this clause will also make an express reference to the data protection obligations set out under Attachment 5 (which includes more restrictive obligations).[53]
Changes to the SLALOM proposed text after feedbacks
N/A
SLALOM proposed text
16.1 Pursuant to this Section 16, the Provider may subcontract any or all of the Services under this Agreement to Subcontractors by giving the Adopter [no less than [X] days'] prior notice which shall include the following information: *(a) the identifying data of the Subcontractor;* *(b) an outline of the proposed subcontracted Services, including: the duration of the subcontract and the quantity or type of Services which will be sub-contracted to the Subcontractor.* *16.2 Subject to Section 16.1 above, the Provider shall:* *16.2.1 remain the Adopter's sole point of contact regarding the Services, including with respect to payment of the Charges.* *16.2.2 not disclose Confidential Information of the Adopter to a Subcontractor unless and until such Subcontractor has agreed in writing to protect the confidentiality of such Confidential Information in a manner substantially equivalent to that required of the Provider under this Agreement.* *16.2.3 not, by virtue of entering into any sub-contract, be relieved of its liability to the Adopter for breach of its obligations under or in connection with the Agreement or otherwise arising from any acts or defaults of its agents and/or subcontractors for which it would otherwise have been liable.*

[53] Cloud Select Industry Group (C-SIG) on Code of Conduct (12 February 2014),

Section 17: Data protection

General description of the Section
Whenever the services offered by the Provider under the agreement involve the processing, including the storage, of personal data (or personal identifiable information, as usually defined under privacy legislations in non-EU countries), as it usually happens, the agreement includes one section which defines the conditions for the processing of personal data and the scope of the related obligations for both the parties. This happens, for instance, whenever the services are used by the Adopter to process personal data of its end users/end customers, if they are individuals (and also a legal entity under certain legislations and/or for some limited purposes, e.g. processing of data in the context of publicly available electronic communications services)[54]. Definition of personal data may vary depending on the applicable data protection and privacy laws and regulations and some jurisdictions and local regulators may restrict the use of cloud services for processing of some categories of personal data (e.g. sensitive data, including health data) if the storage of data is with a third party (e.g. the French legislation - Act n°2002-303 dated 4 March 2002, Decree N°2006-6 of 4 January 2006 and notably Articles 1111-8 and 1111-9 of the French Public Health Code specifically requires that health data are stored with hosting providers accredited with the French Shared Healthcare Information Systems Agency (ASIP)) or outside the EU (e.g. the German legislation is particularly restrictive in relation to transfer of data outside the EU). Processing and/or storing personal data using cloud based services protected under professional rules and secrets may also be subject to restrictions (e.g. lawyers or accountants may want to know who has access to their cloud-stored data since they may be held liable by their own customers). See also Section 4.8.1 of the Deliverable 4.1 / 5.1. Similar provisions on sensitive data stored in the cloud would apply by virtue of the Greek data protection legislation (law 2472/1997 as amended, Opinion 5/2012 of Article 29 data protection WP, etc.) and the non-cloud specific administrative practice adopted by the Hellenic Data Protection Authority (rulings 5/2013, 98/2013. 100/2013, 63/2013 59/2012). Greece has set up (law 3115/2003) a specialized independent authority, for the protection of secrecy in electronic communications by virtue of Article 19 of the Constitution. Such body (in Greek: ADAE) issues specific regulations (165/2011) and acts either alone or jointly with the Data Protection Authority (Ruling 1/2013) for the assurance of confidentiality in internet infrastructures, the protection of internet user confidentiality, network security and resilience (Regulations 165/2011, 205/2013) and so on. ADAE is entitled to perform audits to CSPs, conduct hearings and impose administrative fines in case of non-compliance. Furthermore, in some countries the local data protection authority published (most of them in

[54] On 6th October, 2015 the Court of Justice of the European Union ruled on the adequacy of the measures set forth under the US-EU Safe Harbor (*Maximillian Schrems v. Data Protection Commissioner (Safe harbor – Case C-362/14*))declaring the EU-US Safe Harbor invalid as legal basis to transfer personal data to US. Moreover, on the 22 of September 2015, the Article 29 Data Protection Working Party released an opinion on the C-SIG Code of Conduct on Cloud Computing. . Further to the invalidation of the EU-US Safe Harbor the a new EU-US Privacy Shield has been negotiated at political level between the EU Commission and the U.S. Department of Commerce on February 2nd, 2016; formal approval of the Umbrella Agreement is expected during the 2016, depending on the outcome of the scrutiny of the Article 29 Data Protection Working Party.

2012) recommendations for use of cloud computing services: some of them are more detailed (e.g. the French Data Protection Authority (CNIL)[55], the UK Data Protection Authority (ICO)[56]) than others (e.g. the Italian Data Protection Authority (Garante)[57]), and model clauses for cloud computing contracts. As a matter of fact, in a French contract the following areas would typically be covered, as recommended by CNIL, reporting of security breaches; description of processing means; retention period; audits; clear and complete indication of countries hosting the servers used by the Provider; prohibition of data transfers to a country not providing an adequate level of protection unless a data transfer agreement is signed; informing the Adopter in the case of a request by a foreign administrative or judicial authority; security measures.

A useful reference to be considered when drafting the data protection clauses in cloud service agreements is also the work done by the Cloud Select Industry Group (C-SIG)[58] in the standardization of the Service Level Agreements, and in drafting a Code of Conduct that may be adhered by cloud providers to facilitate demonstrating their compliance with some of their data protection obligations (especially under the GDPR) and to benefit of certain advantages for this.

More important, this clause usually sets out the roles (data controller/data processor) of both the Adopter and the Provider in relation to the personal data stored and/or processed as a result of the services and their primary data protection compliance obligations. Full details of the data processing obligations for the Provider are often part of an attachment to the agreement (this is common in circumstances when the services are offered to EU Adopters or by EU providers)[59].

The GDPR[60], being formally adopted within the first semester of 2016, sets out remarkable changes to the current EU legislation in force on data protection. Although the final document has not yet been published on the EU Official Gazette, it was deemed appropriate to include

[55] Recommendations for companies that intend to subscribe to cloud services (« *Recommandations pour les entreprises qui envisagent de souscrire à des services de Cloud computing* ») available at http://www.cnil.fr/fileadmin/documents/en/Recommendations_for_companies_planning_to_use_Cloud_computing_services.pdf (last access on 5 August 2015).

[56] Guidance on the use of cloud computing (2012) available at https://ico.org.uk/media/for-organisations/documents/1540/cloud_computing_guidance_for_organisations.pdf (last access on 5 August 2015).

[57] Recommendations for companies that intend to use cloud services available at http://194.242.234.211/documents/10160/2052659/CLOUD+COMPUTING+%E2%80%93+PROTECT+YOUR+DATA+WITHOUT+FALLING+FROM+A+CLOUD2.pdf(last access on 5 August 2015).

[58] The C-SIG (https://ec.europa.eu/digital-single-market/en/cloud-computing-strategy-working-groups) was established by the Directorate-General for Communications Networks, Content and Technology, Software and Services, Cloud Unit, with representatives from major European and multinational companies and organizations with significant involvement in cloud computing, for the purpose of providing independent validation and advice on proposals. The C-SIG subgroups' work, including the work done by the Cloud Select Industry Group on Code of Conduct and the Cloud Select Industry Group on Service Level Agreements are working on work

[59] W. Kuan Hon, Cristopher Millard & Ian Walden, *Negotiating Cloud Contracts: looking at clouds from both sides now, Stanford Technology Law Review. Volume 16*, Number 1 Fall 2012, pag. 103 and sub.; European Commission, *Comparative Study On Cloud Computing Contracts, Final Report*, March 2015; European Commission's Expert Documentation.

[60] This document has been drafted taking into account the version of Draft General Data Protection Regulation (2012/0011 (COD)) prepared by the European Council (document dated 11 June 2015 no. 9565/15).

some elements possibly deriving from this new regulation as reasonably expected to be in force starting from middle of 2018.[61]

This section may also refer to a privacy notice given by the Provider to the Adopter in relation to the processing of the Adopter's personal data (especially in case of consumers) to describe how the Provider will process – as data controller for this limited purpose – the Adopter's personal data in order to execute the agreement. However, as this privacy policy may not be required as part of the agreement in many of the jurisdictions (e.g. UK, Germany, Italy), it may be set out in a separate document.

For a picture of some of the current positions from stakeholders and legal experts see Section 4.8 of the Deliverable 4.1/5.1, especially, Section 4.8.2.

Standard clauses used in the market

In the current market practice the Providers adopt different solutions in relation to the data protection topics:

(i) some Providers on the market do not cover the specific data protection related issues in the contractual documentation (especially the role of the parties, or the data location, data availability or data disclosure) and offer only generic details in relation to the security measures they will abide by,

(ii) most of the large Providers do not have a very detailed and comprehensive clause about the data protection topics in the agreement but they prefer to address these topics by distributing them into several clauses or (more often) into the attachments and annexes to the agreement (e.g. the security attachment, and/or the data processing agreement/privacy policy usually available as attachment to the agreement).

Sometimes Providers include specific contractual restrictions and conditions in case the Adopters intend to use their services to process personal data, e.g. the Providers impose a specific obligation onto the Adopters to inform the Provider in case they intend to use the services to process personal data and/or they restrict the Adopters from using the services to process health personal data or legal profession-related personal data.

When coming to data location and data transfer of personal data current market practice by large providers often offers details of the data centres they use to provide the services and are available to offer their services based on specific data location to which the Adopter's data will

[61] The Opinion 02/2015 on C-SIG Code of Conduct on Cloud Computing, dated 22 September 2015 by the Article 29 Data Protection Working Party (WP 232) identifies some interesting recommendations for the C-SIG to be further developed in their Code of Conduct on Cloud Computing, e.g. specific information about the addresses of the locations where processing takes place; introduction of the notion of personal data and anonymization; specific requirements on the issue of transfers or disclosures of data to non EU authorities, based on its interpretation of the proposed Article 43A in the GDPR; prevention from the adoption of terms of services that are to the disadvantage of the clients by unduly limiting cloud providers' obligations and liability and restricting clients' rights; establishing different levels of protection depending on the "processing and the nature of the data to be protected" and to advertise them publicly when offering their services; efforts to implement interfaces between the processors systems and the controller application, so to facilitate a smooth exercise of the audit capabilities realized by the cloud providers; reinforcement of cloud service providers duty, depending on the context, either to provide adequate information to the data subject or cooperate in good faith with their customer to enable him to properly inform data subjects.

be attached; nevertheless, they usually retain the right to move the data from the selected regions to another by notifying the Adopter or, if it is required to comply with the law or request of governmental authorities, also without notification.

It is also common for most of the Providers to mention what are the legal conditions (e.g. use of the Model Clauses based on the EU Commission Decision 2010/87/EU of 5 February 2010 or, until the end of 2015, the Safe Harbor certification[62] and in the next future it will be more common for the Providers to rely on the new Binding Corporate Rules (BCR) for processors) on which the transfer to countries that do not offer adequate protection according to the applicable data protection laws and regulations is based. This may include in the future alternative solutions to the Safe Harbor, e.g. the EU-US Privacy Shield[63] if the new scheme will receive also the approval by the Article 29 Data Protection Working Party.

The security standards applied by the most widely used Providers are often described in detail in the technical attachments to the agreement (especially in case of business to business agreements) or are referred into the agreement by reference to documentation available on the web. In any case in the current market practice most of the Providers undertake to implement "reasonable" security standards (generally the industry market standards in the country/region in which the Provider is based) rather than adhering to specific security standards expressly identified under the legislation of a certain country (e.g. the country of residence of the Adopter). In some instances, and to the extent that this is technically feasible, the liabilities and responsibilities connected with security of personal data and management of the data subjects rights are upheld by the Adopters

Finally, it is also quite common to identify in the documentation referred to in the agreement the undertaking of the Provider (i) to delete personal data up to for maximum period of time (or to store them without any further processing for a certain time) and (ii) to refer to the certification programmes under which they are certified for security and data protection and to offer copy of the annual certification they obtain.

Provider Perspective	**Adopter Perspective**
The Provider is generally interested in achieving high standard of security and protection of the data on one hand, but also in setting out the allocation of responsibilities with the Adopter in such a way to leave on the Adopter a certain number of responsibilities especially in those areas where the allocation of the responsibilities is not clearly defined especially by national data protection rules. Furthermore, sometimes the Providers do	On the other side, the Adopter, in its capacity as data controller, is (or should be) keen to ensure that detailed obligations and instructions are expressly incorporated under the agreement (as reflected under this section and the related annexes to the agreement). This will help to demonstrate control and oversight over the personal data processed and stored under the services. As data controller the Adopter has ultimate responsibility for complying with the data

[62] See Court of Justice of the European Union (*Maximillian Schrems v. Data Protection Commissioner (Safe Harbor – Case C-362/14*) ruling that the US-EU Safe Harbor data transfer agreement is invalid. Most of the providers relying on the EU-US Safe Harbor condition moved to Model Clauses from October 2015; it is also likely that, once the formal agreement on the EU-US Privacy Shield will be reached, these providers will change again their data transfer model to rely on the EU-US Privacy Shield.

[63] http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_eu-us_privacy_shield_en.pdf.

not explicitly refer to their role, in the Agreement, as a Processor as they consider treating their infrastructure as Processors may be inappropriate, or they limit their obligations as they consider they do not have access to data held on their cloud infrastructure and the Adopters remain in control over what data is held and for how long. This is inconsistent with most Adopters' expectations (and guidance from regulators) that the Controller-Processor relationship should be set out in writing wherever relevant (or possibly relevant) to avoid any compliance issues, even if these are viewed as unlikely. Alternatively and more recently, global providers (especially large organisations) tend to offer standardised terms and conditions containing significantly more detailed data protection clauses and obligations and some of them, recently, sought and obtained official confirmation by the Article 29 Working Party, that their data processing contractual documentation for the transfer of personal data in the context of some of their cloud services is in line with the principles set out in the EU Model Clauses approved by the EU Commission Decision 2010/87/EU. This is an attempt to harmonise their exposure to data protection compliance risks throughout the entire region where they offer their services (e.g. Europe vs. Americas).	protection requirements and regulatory guidance possibly issued by competent authorities and is generally required to have in place a "data processing agreement" with the Provider, covering the main data protection related issues (e.g. data location and data transfer, purposes of processing, audit and security obligations including security and data protection incidents notifications, data availability, subcontracting, data deletion).[64]
Position proposed by SLALOM	
The core of this clause will focus on the clear definition of the roles of the parties (setting out by default Adopter/controller and Provider/processor)[65] and the obligation of the parties, but notably of the Adopter, to comply with the applicable data protection legislations and the	

[64] European Commission, *Comparative Study On Cloud Computing Contracts, Final Report*, March 2015. *Opinion 05/2012 on Cloud Computing*, (WP 196) Article 29 Data Protection Working Party; guidance and regulatory constraints (e.g. binding guidance imposed by financial regulators, or domestic legislation imposing restrictions on use of certain cloud providers in specific sectors, for instance France, or guidance released by national data protection authorities, including *Guidance on the use of cloud computing*, Information Commissioner's Office, (2012), *Recommendations for companies planning to use Cloud computing services*, CNIL (2012)) identified by competent authorities.

[65] Suggestion given by the Minutes of the 5th meeting of the Cloud Select Industry Group (C-SIG) on Code of Conduct 12 February 2014.

contractual obligations contained in the agreement (including those outlined under Attachment 5).

The sample below is quite general and should be tailored in such a way to reflect details of the processing actually carried out by the Provider. Indeed, although in many instances the Adopter acts as Data Controller, it is less unusual than expected that an Adopter is a data processor itself in relation to the Personal Data to be processed under the Cloud Service Agreement (e.g. because the Adopter is a payroll service provider offering data processing services to its customers using third party SaaS services). In that case the terms and conditions below require substantial changes to properly reflect the data protection obligations that the Adopter agrees when it negotiates with the Data Controller.

This clause may also provide a sample of privacy notice given by the Provider to the Adopter in relation to the processing of the Adopter's personal data, if applicable(in most countries information related to legal entities, or businesses is not at all – or it is only under very limited circumstances, e.g. in the EU - within the scope of the data protection, or data privacy, laws), describing how the Provider will process – as data controller, for this limited purpose – the Adopter's personal data to execute the agreement.

Changes to the SLALOM proposed text after feedbacks

- We added a drafting note in the Section 17.2 to encourage the drafting parties to enclose specific wording (or reference to other documentation contained in the Agreement or in its annexes) to describe what this monitoring tools are;

- we have slightly amended the Section 17.3 to clarify this is an obligation (and not a warranty) for the Provider, and to adapt the wording to make it potentially more acceptable for the Providers specifying that it is the Providers obligation to implement the security requirements of the applicable Data Protection Laws and Regulations as apply to the Provider in its capacity as a data processor, whilst the Adopter will retain all liabilities in case of breaches caused by the Adopter's failure to its own obligations;

- in line with the changes introduced under Section 17.3, we added a new Section 17.5 to expressly clarify that the Adopter is responsible for any instruction it delivers to the Provider in case they result in omissions or inappropriate actions by the Processor to comply with the data protection laws;

- we slightly simplifies Section 17.6;

- a new Section 17.7 was added to expressly cover the recovery right for the party that paid the compensation to the data subjects on the basis of a joint liability with the other party

- Section 17.8 was slightly supplemented with a warranty to be given by the Adopter about having obtained valid consent from the Data Subjects, if so required by the law, to have their Personal Data processed for the purpose of the agreement.

SLALOM Section

17.1 Under this Agreement, the Adopter qualifies as Data Controller of the set of Processing carried out by the Provider on his behalf. The Provider qualifies as Data Processor upon

signature of this Agreement and will remain as such as long as it (i) complies with the Adopter's reasonable and legitimate instructions, including the instructions set out under Attachment 5 to this Agreement, (ii) provides adequate monitoring procedures regarding compliance with such instructions, (iii) does not go beyond the mandate given by the Adopter by acquiring a relevant role in determining the purposes or the essential means of Processing.

17.2 The Provider shall provide an accessible, easy-to-use and comprehensive security-monitoring-tool [Note: where appropriate, it is possible to include a description of the tool or referring to a description of the tool to be attached to the Agreement]. The Adopter is fully liable for data protection law compliance. Therefore, the Adopter must comply with the applicable Data Protection Laws and Regulations, especially, but not limited to, requirements to ensure that the Processing of Personal Data complies with the applicable legislation in relation to the nature of the Personal Data and formal requirements with the local data protection authorities in relation to the transfer of Personal Data.

17.3 The Provider acknowledges and agrees that it has appropriate experience and capabilities, and will implement appropriate technical and organizational measures, to ensure that the Processing of Personal Data by the Provider in the course of providing the Services will meet such requirements of the applicable Data Protection Laws and Regulations as apply to the Provider in its capacity as a Data Processor, provided always that the Adopter acknowledges and agrees that the Provider shall not be in breach of this clause 17.3 where any failure to comply with Data Protection Laws and Regulations is caused by or results from the acts or omissions of the Adopter, its officers, employees or agents. The Provider acknowledges that failure to meet the obligation under this clause 17.3 will be deemed to be a material breach of this Agreement for the purposes of Section 9.2.

17.4 The Adopter shall remain liable for the damage which a Data Subject may suffer as a result of the Processing of Personal Data which is under its control and is not resulting from a breach by the Provider of its obligations under this Section 17.

17.5 The Adopter further acknowledges that the Provider is reliant on the Adopter for lawful direction and instructions as to the extent to which the Provider is entitled to process any Adopter Personal Data and, consequently, the Adopter agrees that the Provider will not be liable – and it will indemnifies the Provider - for any claim brought by a Data Subject arising from any action or omission by the Provider, to the extent that such action or omission resulted directly from the Adopter's lawful instructions.

17.6 The Provider will remain fully liable in case of any breach of its direct obligations under this Agreement and the applicable Data Protection Legislations and Regulations with respect to the Processing of Personal Data validated under this Agreement, including failure to act in accordance with lawful instructions of the Adopter and where any such breaches are caused by any subcontractor engaged in compliance with the requirements set forth under this Agreement.

17.7 Each of the Parties acknowledges and agrees that, where the Adopter or the Provider has paid full compensation for the damages suffered by a Data Subject, where a joint liability has been ascertained in the course of a proceeding, the Party that fully indemnified the Data Subject is entitled to claim back from the other Party that pro rata of the compensation corresponding to the its part of responsibility for the damage as resulting

from the final court decision.

17.8 *[ONLY APPLICABLE IN CASE THE ADOPTER IS A CONSUMER/INDIVIDUAL OR IN CASE OF PROCESSING OF ELECTRONIC COMMUNICATION SERVICES. ANY SUCH NOTICE, IF REQUIRED UNDER THE APPLICABLE DATA PROTECTION LAWS AND REGULATIONS CAN BE SET OUT AS SEPARATE DOCUMENT. THE FOLLOWING IS ONLY A GENERIC EXAMPLE OF SUCH A NOTICE]*

In case of any Personal Data related to the Adopter, its officers, employees or agents, if applicable, the Provider and its staff will hold and Process, mainly using electronic devices, their Personal Data to execute and perform this Agreement (including management of administrative related matters, maintaining records, administering accounts receivable, fulfilling social security and tax obligations [to add other purposes, if applicable]. The Provider will implement appropriate security measures in line with those specified under Attachment 6 to this Agreement. The Adopter acknowledges that providing those Personal Data is necessary for the execution and administrative management of this Agreement and that the Personal Data may be shared by the provider with [to list the categories of Third-Parties, including service providers, sharing the Adopter's information with the Provider]. Where necessary for the purposes above, Personal Data may be transferred to a country or territory outside the European Economic Area [to list, if possible, countries of transfer and the reasons for the transfer], in accordance with the applicable Data Protection Laws and Regulations. Upon request, the Adopter, its officers, employees and agents are entitled to obtain access to and to supplement and rectify their Personal Data with the Provider and, on legitimate grounds, to object in writing to the processing of their Personal Data, emailing or contacting the Provider at the contact addresses under Section 19 below. If so required under the applicable Data Protection Laws and Regulations, by signing this Agreement the Adopter (i) consents, and warrants that it has the authority to consent, to the Provider collecting, using and disclosing the Adopter's, and (ii) warrants that it has obtained all necessary consents from the relevant Data Subjects, including its officers, employees and agents, and is entitled to transfer the relevant Personal Data to the Provider so that the Provider may lawfully use, Process and transfer the Personal Data in accordance with this Agreement on the Adopter's behalf.

Section 18: Force majeure

General description of the section
This provision sets out the obligations of the parties in circumstances where, due to events outside either parties' control, the performance of the services/obligations cannot be achieved. The section may, for instance, include a suspension right which could delay the services for the duration of the above event[66]. This application of this provision has an impact on the application of the SLA. Accordingly, it is

[66] Article 1218 of Italian Civil Code: "The debtor who does not exactly render due performance is liable for damages unless he proves that the non-performance or delay was due to impossibility of performance for a cause non imputable to him".

important to understand if and how the SLA can be derogated in a force majeure event occurrence.

Standard clauses used in the market

Generally, the cloud computing agreements set forth that if there is any event which is not under the control of the Providers, they will be not responsible for the delay or failure to provide the services.

In most of the cases, the cloud computing agreements provide also some examples which can be considered as force majeure events (only by way of example) such as earthquake, storms, riots, acts or orders of government, acts of terrorism, disturbance, rebellion, strike, lock-out or labour dispute.

No similar provision is contained in the above cloud computing agreements with reference to the Adopter.

Provider's perspective	**Adopter's perspective**
The Provider will be concerned to ensure that force majeure covers a wide range of cases (i.e.: events which are not under its control) since it will not be obliged to fulfil its obligations and to provide the services according to the service level agreement.	It is very important for the Adopter to clarify the relationship between the force majeure events and the possible services of disaster recovery and business continuity, if any. If provisions relating to business continuity or disaster recovery have been provided, the Adopter will want assurances that, in the event of a force majeure event, the services can still be performed, in accordance with the terms of those systems. The Adopter will also want an ability to terminate the cloud computing agreement, where a force majeure event exceeds a specified length of time.

Position proposed by SLALOM

This section shall set out specific events which could trigger force majeure and shall clearly reference the business continuity and disaster recovery obligations of the Agreement as detailed in its attachments.

If such events are not covered by the disaster recovery or business continuity plan, the Parties shall be entitled to terminate the CSA, or the affected Services, if the force majeure event exceeds a specified period of time. Otherwise, the Parties will remain bound by the terms of the CSA.

Changes to the SLALOM proposed text after feedbacks

N/A

SLALOM proposed text

18.1 If a Force Majeure Event occurs which prevents a Party (the "Affected Party") performing any of its obligations hereunder or causes a delay in performance, the Affected Party shall not be liable to the other Party and shall be released from its obligation to fulfil its obligations under

this Agreement to the extent that its ability to fulfil such obligations has been directly affected by the Force Majeure Event, provided that:

18.1.1 the Affected Party notifies the other Party in writing as soon as reasonably practicable of the occurrence of the Force Majeure Event and the nature and likely duration of its impact upon the other Party;

18.1.2 the Affected Party takes all reasonable steps to mitigate the impact of the Force Majeure Event on the other Party, and in particular continues to perform those obligations affected by the Force Majeure Event but whose performance has not been rendered impossible to the highest standard reasonably practicable in the circumstances;

18.1.3 the Affected Party continues to perform all its obligations which have not been affected by the Force Majeure Event; and

18.1.4 the Affected Party resumes normal performance of all affected obligations as soon as the impact of the Force Majeure Event ceases, and notifies the other Party in writing promptly of such resumption.

18.2 If the impact of the Force Majeure Event upon the Affected Party continues for a period of no less than [to be provided] consecutive days the Affected Party may, without incurring liability, terminate this Agreement either in whole or in part with immediate effect by providing written notice to other Party, without having to file a claim with the competent Court to that effect.

18.3 The Parties agree that, if the Affected Party is the Provider, in respect of the period during which any Force Majeure Event subsists, the Adopter shall not be required to pay the Charges relating to those Services which cannot be performed as a result of the Force Majeure Event, and in respect of those Services which are affected by the Force Majeure Event but can be performed, shall be required to pay an amount which reasonably reflects the standard to which those Services were provided during such period.

Section 19: Notices – Parties' team leaders

General description of the section
This section relates to the process by which communications are exchanged between the parties. The section will also set out the names of the persons responsible for managing the contract. The section does not raise any particular legal issues, however, in case of a dispute between the parties concerning the performance of any obligations of the agreement, it could be important to know (and be able to prove) if a specific communication has be sent to the right person. Being able to clarify who the point of contact is for the communications also gives the parties some certainty on this point. With reference to cloud computing agreements executed in internet these data are normally provided and/or shared in the subscription process.

Standard clauses used in the market

In some cases, the cloud computing agreements set out that the communications sent by the Provider are effective upon posting them in the website.

In case the communications are sent via email, the cloud computing agreements provide that they are effective when the Provider has sent them.

It is therefore responsibility of the Adopter to check the relevant webpage on its cloud account or its email to see if any communication has been sent.

Some cloud computing agreements also provide the language of the communication.

In some other cases, the cloud computing agreements provide that the notice must be sent by the Adopter in writing (being the email considered as written communication) and specify the office or contact to be addressed.

Provider's perspective	**Adopter's perspective**
The Provider and the Adopter do not have any different perspectives on these provisions in general.	

Position proposed by SLALOM

From an operational perspective, confirmation of the names of the people responsible for managing the contract will be important. Moreover, it is also important to ensure that all communications between the Parties are sent by in writing by email (i.e. no verbal communications) save in case particular other requirements are provided in the contract for special communications.

If the SLALOM CSA will be executed by internet the data and information on Teams Leaders (or competent office of the Provider) may be shared during the electronic subscription process.

Changes to the SLALOM proposed text after feedbacks

1) We provided that an email is deemed to have been served at the time and date certified by the delivery confirmation in lieu of the date and timing of sending if in working hours. This change should guarantee more than before the certainty of the communication by email, as this should be the main communication mean used by the parties.

SLALOM proposed text

19.1 Except as expressly provided elsewhere in this Agreement, any notice to be given under this Agreement, refer to the Agreement and to the respective team's leaders.

19.2 The Parties' respective representatives for the receipt of notices in relation to the Agreement are, until changed by notice given in accordance with this clause, as follows:

For the Provider: [●]

Providers' Team Leader: [●]

Email: [●]

Telephone: [●]

Fax: [●]

Address: [●]

For the Adopter: [●]

Adopter's Team Leader: [●]

Email: [●]

Telephone: [●]

Fax: [●]

Address: [●]

19.3 The Provider's Team Leader and the Adopter's Team Leader, as defined in Section 19.2 above, shall be responsible for the co-ordination of all matters relating to the Services and the execution of this Agreement.

19.4 Any change of the Provider's Team Leader or the Adopter's Team Leader shall be previously communicated in writing to the other Party to be effective.

19.5 Any notice shall be deemed to have been served:

19.5.1 if delivered by hand, at the time and date of delivery;

19.5.2 if sent by recorded delivery or registered post, forty-eight (48) hours from the date of posting (such date as evidenced by postal receipt etc.);

19.5.3 if sent by e-mail, at the time and date certified by the delivery confirmation; and

19.5.4 if sent by registered airmail, five days from the date of posting.

Section 20: Governing law

General description of the section
This clause sets out the governing law of the cloud computing agreement. According to Section 3 of European Regulation 593/2008 (directly applicable in all Member States), the parties are entitled to choose the governing law of the contract[67]. With reference to consumer contracts, according to Article 6 of above EU Regulation such contracts shall be governed by the law of the country where the consumer has his habitual residence provided that the professional: (a) pursues his commercial or professional activities in the country where the consumer has his habitual residence, or (b) by any means, directs such

[67] Fabio Bortolotti, *Diritto dei Contratti Internazionali*, Cedam, pag. 306.

activities to that country or to several countries including that country, and the contract falls within the scope of such activities.

Generally, under German law, providing that, should the Adopter be a consumer, any choice of law shall apply only to the extent permitted by law, does no substantial harm to the Provider's position.

Under Italian law, the choice of a foreign law will not prejudice the application of many provisions protecting the consumers[68].

Regardless of the Adopter's classification as a consumer or a business and regardless of any choice of law, where permitted, the parties should be clear that the data protection requirements and related obligations might be governed by a law other than the governing law, given the fact that generally, at least in Europe, the applicable data protection law is based on the country where the Adopter (as controller) is established.

Standard clauses used in the market

According to most cloud computing agreements, it is common providing the law of a specific country which may apply to the agreement. This choice in most of the cases is made by the Providers.

In limited cases, however, the clause at issue provides that the governing law is the law of the country in which the Adopter is domiciled.

Provider's perspective	**Adopter's perspective**
The Provider would be keen to ensure that the governing law of the country in which has its registered office or its headquarters. In some other cases, the Provider could prefer (e.g.: for tax reasons) to provide the governing law applicable in the country where other legal entities of its group have their registered office.	The Adopter would be keen to ensure that its own governing law is stated. As a second option it could propose a governing law which is different from the law of its country or from the law proposed by the Provider.

Position proposed by SLALOM

In the proposed SLALOM model CSA the Parties can choose which governing law will apply. In other words the Parties should be free to choose such law, being clear that the governing law may be different from the position under data protection law and that many provisions of law protecting the consumers under the applicable legislation of the their country will apply.

We exclude the application of the United Nations Convention on Contracts for the International Sale of Goods and the 1974 Convention on the Limitation Period in the International Sale of Goods, which otherwise might automatically apply to cloud computing services.

[68] Italian Code of Consumers (legislative decree 206/2005); Articles 36, para 5 and 143, para 2.

Changes to the SLALOM proposed text after feedbacks
N/A
SLALOM proposed text
20.1 This Cloud Service Agreement and any dispute or claim arising out of or in connection with it or its subject matter or formation (whether contractual or non-contractual, including tort, breach of statute or regulation or otherwise) shall be governed by and construed in accordance with the legislation of [to be provided]. In case the Adopter is a consumer, the above choice of the law shall apply to the extent permitted by the applicable law. The present Section 20.1 shall apply without prejudice to the mandatory applicable data protection legislation. *20.2 The parties expressly reject any application to this Cloud Service Agreement of (a) the United Nations Convention on Contracts for the International Sale of Goods, and (b) the 1974 Convention on the Limitation Period in the International Sale of Goods, as amended by that certain Protocol, done at Vienna on April 11, 1980.*

Section 21: Disputes - jurisdiction

General description of the section
The clause concerns: i) how the parties will deal with possible disputes outlining process by which disputes may be resolved, ii) if the above process has not resolved the dispute, the section will set out the name of the competent court by the parties. According to Section 21, para 1 of the Regulation 44/2001, the parties may choose the competent court in case of disputes[69], save where the Adopter is a consumer[70]. With reference to agreements with consumers EU Regulation 44/2001 (Article 16), provides that: "*1. A consumer may bring proceedings against the other party to a contract either in the courts of the Member State in which that party is domiciled or in the courts for the place where the consumer is domiciled.* *2. Proceedings may be brought against a consumer by the other party to the contract only in the courts of the Member State in which the consumer is domiciled*". Any choice about the

[69] "*1. If the parties, one or more of whom is domiciled in a Member State, have agreed that a court or the courts of a Member State are to have jurisdiction to settle any disputes which have arisen or which may arise in connection with a particular legal relationship, that court or those courts shall have jurisdiction. Such jurisdiction shall be exclusive unless the parties have agreed otherwise. Such an agreement conferring jurisdiction shall be either:*
(a) in writing or evidenced in writing; or
(b) in a form which accords with practices which the parties have established between themselves; or
(c) in international trade or commerce, in a form which accords with a usage of which the parties are or ought to have been aware and which in such trade or commerce is widely known to, and regularly observed by, parties to contracts of the type involved in the particular trade or commerce concerned".

[70] Fabio Bortolotti, *Diritto dei Contratti Internazionali*, Cedam, pag. 442.

competent court will not affect the mandatory jurisdiction provided for data protection related disputes under the applicable data protection law[71] [72].

Under French law, no claim can be filed with a Court until the amicable resolution process/ mediation has been completed and has failed[73]. However, the escalation process and, as the case may be, the mediation process should not prevent any party from taking legal action to obtain interim measures or injunctive relief ("*mesures provisoires ou conservatoires*") for instance in case of unfair/illegitimate suspension of services/ need to recover the data/ security breaches etc.

According to French law, as a general principle, where a dispute is to be heard by a National Court, it is always better to have an agreement drafted in such language. If not feasible, a French Court will likely request that the contract be translated. In these circumstances, it might be better to reach an agreement on the translated version beforehand and a precedence clause may not be needed

For consumer contracts, the agreement has to be drafted in French as a mandatory requirement (Use of French Language Act n° 94-665 of 4 August 1994).

According to German law, providing that, should the Adopter be a consumer, any choice of competent jurisdiction shall apply only to the extent permitted by law, does no substantial harm to the Provider's position.

Greek law also provides for mediation (e.g. Consumer Ombudsman) or arbitration. Should those non-compulsory mechanisms of alternative dispute resolution fail, parties may refer the case before the competent national courts, as per the Code of Civil Procedure, depending on the type of the dispute, the choice of law contract provisions, the location and the legal seat of each party. Interim or precautionary measures are also possible for cloud contracts under procedural Greek law.

In accordance with the Italian law (Article 1341 of the Italian Civil Code), the choice of the competent court may be considered as a burdensome clause. If such burdensome clause is provided in a standard agreement drafted by one of the party, such clause (mentioned by its name and number) needs to be specifically approved in writing by the counterparty (even if it is not a consumer). If not specifically approved, the clause will be void. Such written approval may not be given by electronic means unless a digital signature (i.e.: kind of advanced electronic signature) is used, but only with a signature on the hardcopy of the agreement.

Standard clauses used in the market

The clause concerning the jurisdiction in most of the cases provides the competent court for possible disputes.

Different competent courts may be provided depending on the value of the dispute, or on the identity of the Adopter (for instance if it is country or state entity, or a consumer).

[71] Directive 95/46/EC (Article 22) and European Convention of Human Rights (Articles 34–37).
[72] Draft of EU General Data Protection Regulation (Articles 75 and 77).
[73] Paragraphs 7 of Article 56 and Article 58 of the French Code of Civil Procedure

In very limited cases, the cloud computing agreements provides that the applicable jurisdiction varies depending upon where the customer is domiciled or do not provide any applicable jurisdiction.	
Provider's perspective	**Adopter's perspective**
The Provider will be keen to ensure that the competent court for any dispute relating to the cloud computing agreements shall be referred to a court of the country where the Provider has its headquarters.	The Adopter will be interested to ensure that the competent court is the one where the contracting party of the Adopter has its office
Position proposed by SLALOM	
The proposed SLALOM model CSA shall provide a process for the amicable resolution of the dispute with an escalation procedure if the dispute becomes protracted. We will leave a blank for the competent court (save where the proposed SLALOM model CSA deals with consumers).	
Changes to the SLALOM proposed text after feedbacks	
1) For sake of clarity, we provided a specific provision for injunctive or other emergency or interim relief establishing that amicable procedure of Section 21.1 and the final choice of the competent court shall not prevent either party from taking such action as it deems appropriate (including any application to a relevant court) for injunctive or other emergency or interim relief.	
SLALOM proposed text	
21.1 Without prejudice of Section 21.2, if any dispute should arise between the Parties relating to or deriving from this Cloud Service Agreement, it may be settled in the first instance in accordance with the following procedure: *(i) when a dispute arises, one Party may request the other in writing to start the settlement procedure;* *(ii) the Parties undertake to appoint their own representative, holding suitable powers, selected from persons who are not directly involved in the performance or management of this Cloud Service Agreement and the corresponding activities; the said Parties' representatives shall meet with the aim of settling the dispute amicably, having regard above all to the primary need to maintain the continuity of the Services forming the subject of this Cloud Service Agreement;* *(iii) if, after making all reasonable attempts at a settlement, the said representatives are unable to settle the dispute within 30 (thirty) days of the date of the request to initiate the settlement procedure, either Party may refer the dispute to the court as stated in Section 21.2 hereof.* *21.2 The procedure of Section 21.1 shall not prevent either Party from taking such action as it deems appropriate (including any application to a relevant court) for injunctive or other emergency or interim relief.* *21.3 The Parties irrevocably agree that the Court of [to be provided] shall have exclusive*	

jurisdiction to settle any dispute or claim that arises out of or in connection with this Cloud Service Agreement or its subject matter or formation (including non-contractual disputes or claims). In case the Adopter is a consumer, the above choice of the competent court shall apply to the extent admitted by the applicable law.

Section 22: Final provisions

General description of the Section	
These provisions tend to deal with general 'boilerplate' provisions.	
Standard clauses used in the market	
These kind of clauses are normally provided in most of the agreements with very few changes from one agreement to another.	
Provider's perspective	**Adopter's perspective**
The parties will tend to adopt a similar approach to these provisions.	
Changes to the SLALOM proposed text after feedbacks	
N/A	
Position proposed by SLALOM	
The following standard clauses commonly used in international contracts are set out here. With reference to the assignment of the Agreement, we will provide the right of either party to assign it to other entities of the same Group. Under German law a severability clause would have no effect, even if it is quite commonly used. The court would apply straight away statutory law in lieu of an unenforceable/invalid provision. Under Italian law the severability clause generally used in international contracts could be considered not in line with Article 1419, para 1, of Italian Civil Code which states that if a clause is declared void, the validity of the agreement would not be affected unless it can be proved that the parties would have not executed the agreement without such clause.	
SLALOM proposed text	
22.1 ***Assignment****: Neither Party may assign to Third-Parties the present Cloud Service Agreement without prior consent of the other Party. The consent of the Party will not be unreasonably withheld. Either Party shall have the right to assign any or all of its rights and obligations under this Cloud Service Agreement in whole or in part to its Group or to the successor to the whole or a part of Party's business, subject to such entity or successor undertaking in writing to the other Party that it will perform all assigning Party's obligations under this Cloud Service Agreement*.	

22.2 ***Entire Agreement****: This Cloud Service Agreement (together with all other documents to be entered into pursuant to it) sets out the entire agreement and understanding between the Parties, and supersedes all proposals and prior agreements, arrangements and understandings between the Parties, relating to its subject matter.*

22.3 ***Language****: In case of discrepancy between the English language original text of the Agreement and other language translation, the English text shall prevail.*

22.4 ***No partnership or agency****: Nothing in this Cloud Service Agreement shall be deemed to constitute a partnership between the Parties, nor constitute either Party the agent of the other party for any purpose.*

22.5 ***Third Party****: A person who is not a Party to this Cloud Service Agreement shall not have any rights to enforce any term of this Cloud Service Agreement, but this does not affect any right or remedy of a Third Party which exists, or is available, apart from that Cloud Service Agreement.*

22.6 ***Severability:*** *If any term of this Cloud Service Agreement is or becomes illegal, invalid or unenforceable in any jurisdiction, that shall not affect:*

22.6.1 *the legality, validity or enforceability in that jurisdiction of any other term of this Cloud Service Agreement; or*

22.6.2 *the legality, validity or enforceability in other jurisdictions of that or any other provision of this Cloud Service Agreement.*

22.7 ***Amendments:*** *Any amendment of this Cloud Service Agreement shall not be binding on the Parties unless set out in writing, expressed to amend this Cloud Service Agreement and signed by authorised representatives of each of the Parties.*

22.8 ***Waiver:*** *Delay in exercising, or failure to exercise, any right or remedy in connection with this Cloud Service Agreement shall not operate as a waiver of that right or remedy. The waiver of a right to require compliance with any provision of this Cloud Service Agreement in any instance shall not operate as a waiver of any further exercise or enforcement of that right and the waiver of any breach shall not operate as a waiver of any subsequent breach. No waiver in connection with this Cloud Service Agreement shall, in any event, be effective unless it is in writing, refers expressly to this clause, is duly signed by or on behalf of the party granting it and is communicated to the other party.*

Section 23: Attachments

General description of the Section
These documents are to be attached to the agreement. They have to set out the scope of the contractual relationship between the Provider and the Adopter. The attachments have to be connected and coordinated with the agreement which have to specifically recall and refer to them to make them effective, enforceable and connected with all

other provisions of the agreement.
Standard clauses used in the market
The cloud computing agreements executed in internet normally refer to other webpages provided in the same website.

Provider's perspective	**Adopter's perspective**
The parties tend to adopt a similar approach to these provisions.	

Position proposed by SLALOM
We will provide a typical list of the Attachments which are commonly provided together with the CSA. If the SLALOM Agreement will be executed by internet, the Attachments will be published in separate webpages referred to in the CSA.
Changes to the SLALOM proposed text after feedbacks
N/A
SLALOM proposed text
23.1 The following Attachments are an integral part of this Cloud Service Agreement: *23.1.1 Attachment 1: Services Description;* *23.1.2 Attachment 2: Service Level Agreement;* *23.1.3 Attachment 3: Acceptable Use Policy;* *23.1.4 Attachment 4: Consideration;* *23.1.5 Attachment 5: Data Protection* *23.1.6 Attachment 6: Security.*

Attachment 1 to the Agreement: Services Description

Description of the SLALOM Attachment
This Attachment will provide a description of the Services that the Provider is committed to provide under Section 2 of the Agreement.

SLALOM Introduction of this Attachment
The Provider shall provide to the Adopter the Services detailed in this Attachment 1.

Attachment 2 to the Agreement: Service Level Agreement – Service Credits

Description of the SLALOM Attachment
This Attachment shall provide the Service Levels and the Service Level Objectives of the Services in accordance with Section 3 of the Agreement. The Service Levels are detailed in Deliverables D3.1 Initial Position Paper (technical), D4.1/5.1 Initial Position Paper (Provider and Adopter's perspectives). In connection with the Service Levels and the Service Level Objectives the Parties shall agree the Service Credits.
SLALOM Introduction of this Attachment
The Provider shall, during Term, fulfil the Service Level Agreements detailed under the present Attachment 3, in accordance with Section 3 of the Agreement.

Attachment 3 to the Agreement: Acceptable Use Policy (AUP)

Description of the SLALOM Attachment
The Attachment 2 to the Agreement will provide the Acceptable Use Policy as provided under Section 5 of the Agreement The Acceptable Use Policy of SLALOM concern the following main issues: 1) IPR rights (of the Provider or Third Party) 2) Illegal activities; 3) Security of the Provider; 4) Data Protection rights. We have not received feedbacks by the stakeholders on this Attachment.
SLALOM Acceptable Use Policy
ACCEPTABLE USE POLICY *In accordance with Section 5 of the Agreement, the Adopter shall comply with the following terms of use of the Services:*

- ***While using the Services, the Adopter SHALL NOT:***

  1) infringe any Third Party's Intellectual Property Rights;

  2) infringe Providers' Intellectual Property Rights;

  3) breach any applicable law, regulations and order of the authorities;

  4) process Third Party's Personal Data illegally;

  5) breach any other Third Party's rights which are different from above points 1) and 4);

  6) upload or introduce malicious code, viruses, trojan horses, e-mail bombs, spyware, malware, and other similar software;

  7) allow Third-Parties external to the Adopter's organization to use the Services unless authorised in writing by the Provider;

  8) send unsolicited e-mail or communications of any kind;

  9) support in any way illegal activities;

  10) misrepresent or obscure the identity of the Adopter's users;

  11) upload illegal Contents on the System;

  12) violate any applicable export and re-export control legislation and regulations;

  13) upload or introduce encryption software in violation of national and international exporting legislation;

  14) use means which can cause a breach of security of the Provider's equipment;

  15) use means which can cause a disruption of the Services.

- ***While using the Services, the Adopter SHALL:***

  16) adopt secure id and passwords in relation to the access to the System in line with any possible instructions provided by the Provider;

  17) inform the Provider in case of loss of the id and passwords for accessing the Services not later than 3 (three) Working Days from the discovery;

  18) inform the all Adopter's Users (employees, officers, consultants) of the terms and conditions of the AUP;

  19) process Personal Data of Third-Parties in accordance with the applicable legislation (e.g. , if so required under the applicable law, provide full notice to the Data Subjects and obtain their valid consent, notify the Processing of Personal Data with the competent data protection authority, implement any security measures on its side of the Service to ensure full compliance with the legislation, monitor the Services);

20) obtain the consent of the owners of the Intellectual Property Rights to use their works on or through the Services.

Attachment 4 to the Agreement: Charges

Description of the SLALOM Attachment
This Attachment shall provide the Charges payable by the Adopter to the Provider for the provision of the Services according to Section 6 of the Agreement.
SLALOM Introduction of this Attachment
In accordance with above Section 6 of the Agreement, the Adopter shall pay to the Provider the amounts detailed under the present Attachment 4 in accordance with the following terms and conditions.

Attachment 5 to the Agreement: Data Processing Attachment

Description of the SLALOM Attachment
This attachment is intended to cover the data protection rules governing the processing of personal data processed by the Parties under the Cloud Service Agreement. In most countries the Adopter should be made aware of how the process works, who operates the data centres and who has access to them, and the fact that unlimited copying of data in long sub-processing chains is likely to be considered by the courts and regulatory authorities in some countries (e.g. Greece) as a major privacy risk. It is not possible, typically, to identify by default the Adopter as Data Controller of the Personal Data under the Cloud Service Agreement, even though this often reflects the scenarios on the market. Sometimes the Adopter is a Data Processor itself, and in that case the terms and conditions below cannot apply as is, but require to be amended to properly reflect the data protection obligations that the Adopter agrees when it negotiates with the Data Controller (e.g. the Adopter's customer/final user). For the purpose of this Deliverable D2.2, the scenario described below ideally applies to Adopters entering into the Cloud Service Agreement as Data Controllers. Although the Adopter, acting in the capacity of Data Controller, typically has the main interest in ensuring compliance with the applicable Data Protection Legislation and Regulations and drafting this attachment in sufficient detail, it is also in the interests of the Provider to clarify how responsibilities are shared between the Parties. Directive 95/46/EC, and the GDPR[74] requires the Data Controller (or cloud computing users) to enter into a written agreement with the data processor governing the Provider's obligations and/or prohibitions regarding Personal Data processing and the Adopter's obligations.

[74] See note no. 2.

Attachment 5 to the Agreement will provide detailed rules governing:

a. Definition of categories of personal data.

b. The Adopter's responsibility as Data Controller: the Adopter, acting in the capacity of Data Controller, must accept responsibility for complying with all applicable Data Protection Legislation and Regulations.

c. Purpose limitation: the Provider is entitled to process Personal Data only within the scope of the Services, and is prohibited from using the Personal Data for any independent or additional purpose not required for the provision of Services, including a prohibition on sharing data with Third Parties unless a legitimate interest or any other justifications provided by the applicable Data Protection Legislation and Regulations apply. For information about some of the current concerns on the market and at institutional level regarding possible secondary use of personal data by the Providers, see Section 4.8.1 of Deliverable 4.1 and 5.1.

d. Subcontracting: the Provider's obligations are as follows:

- to inform the Adopter and obtain its consent if Third Parties or Subcontractors (whether based abroad or not) are used to perform operations relating to the Services, and to identify them to the Adopter. The Adopter's consent will usually be given, with the proviso that the Provider is obliged to inform the Adopter (a Data Controller) of any intended changes. The Adopter, however, retains the right to object to such changes or to terminate the Cloud Service Agreement;
- to impose on these Third Parties similar obligations in relation to their contracts addressing how Personal Data will be protected and to what extent the Third Party is liable; and
- to put in place procedures allowing Data Subjects to exercise their rights (rights of access, alteration or deletion, etc.).

e. Cooperation obligations between the Provider and the Adopter, including the Provider's obligation to cooperate with the Adopter to give the Adopter all useful information about the processing of Personal Data, also for the purpose of demonstrating compliance with the obligations laid down under the Data Protection Legislations and Regulations and of notifying the competent data protection authority where required by the applicable Data Protection Legislation and Regulations, and to cooperate with the competent data protection authorities, when requested.

f. Notification obligations: the Provider shall notify the Adopter of any security breach and any law enforcement act requiring the Provider to grant access to Personal Data (unless this is prohibited by the applicable legislation, e.g. secrecy obligations relating to criminal investigations). For information about some of the current positions taken by stakeholders and legal experts, see Sections 4.8.2.2 and 4.8.7.1 of Deliverable 4.1 and 5.1.

g. Data transfer: data location is closely linked to matters such as law enforcers' access, data security and transparency. It is important to establish not only where Personal Data are located but also from where Personal Data are accessible and who guarantees the security of the cloud Service. Moreover, data location is important to determine the applicable law and to define the risks. Knowing where the infrastructure is located (e.g. to be provided at a list of locations) or the structure of the Provider is more important than the exact location of the data at a specific time (e.g. in the event of an e-discovery procedure). In practice, the Cloud Service Agreement must outline the Provider's obligations:

- to inform the Adopter of all locations in which data may be stored or processed by the Provider and/or its subcontractors (notably, if some or all locations are outside the European Economic Area); and

- to ensure adequate protection for data transfer outside the EEA (e.g. by means of the EU Model Clauses, Binding Corporate Rules ("BCR") or alternative means approved at EU level). For information about some of the current positions taken by stakeholders and legal experts, see Section 4.8.7.3 of Deliverable 4.1 and 5.1. h. Security measures: most of the applicable Data Protection Legislation and Regulations require Data Controllers to implement adequate security measures. In some countries (e.g. Italy – primarily Sections 31-35 and Annex B to the Italian Data Protection Code – and Germany – Sections 9 and 11 of the German Federal Data Protection Act, and also Greece, which requires, among other things, specific training for staff about the confidentiality, integrity and availability of personal data and information systems, availability of systems according to Service Level Agreements, installation of services properly partitioned and configured to ensure contractual obligations are met, and encryption) the Data Protection Legislation and Regulations also detail the main security measures that must be implemented when processing Personal Data, and these security requirements must be detailed in the agreement (or in any attachment thereto, e.g. the security or data processing attachment). The data processing attachment also needs to detail the Provider's obligation to ensure that the processing complies with the applicable security measures and to implement physical, technical and organisational safeguards accordingly to ensure the availability, integrity and confidentiality of the Personal Data (including via a cross-reference to security-focused sections and attachments to the agreement, covering, among other things, traceability, e.g. traceability of users' operations and anomalies, and continuity of services, backups and integrity, e.g. backup system, redundancy of servers, etc.). For additional evaluations of security issues, please refer to Sections 4.17 and 4.18 of Deliverable 4.1 and 5.1. h. Audit: the Adopter is entitled to audit the Provider to ensure that the Provider is processing Personal Data in compliance with the applicable Data Protection Legislation and Regulations. i. Certifications: proof of relevant certifications, if any, by independent qualified auditors of the Provider's services according to the most relevant national and international standards (e.g. ISO/IEC 27001, ISO/IEC 27018 and any upcoming standard for cloud computing, e.g. ISO/IEC 19086). The Adopters may also negotiate to obtain a copy of the certification report relevant to the Services, provided that they comply with the applicable confidentiality obligations. See also the comments on this point under Section 4.9.3 of Deliverable 4.1 and 5.1. j. Deletion of data: the Provider shall erase (and have its subcontractors erase) personal data from wherever they are stored as soon as they are no longer necessary for the specific purposes, i.e. after the agreed maximum retention time (including back-up needs) during the course of the agreement, and in any event after a fixed maximum period agreed by the parties after termination of the Cloud Service Agreement.
Slalom Introduction of this Attachment
This Data Processing Attachment ("DPA") is made a part of the Cloud Service Agreement between the Adopter and the Provider to reflect the Parties' agreement with regard to the Processing of Personal Data as specified under the Cloud Service Agreement and all documents, attachments and exhibits incorporated therein, in accordance with the requirements of the applicable Data

Protection Legislation and Regulations, and especially for the purpose of Section 17 of Directive 95/46/EC, as amended or replaced from time to time[75], as applicable.

This DPA is subject to the terms of the Cloud Service Agreement and is annexed as an attachment to the Cloud Service Agreement. In the event of any conflict between the terms of the Cloud Service Agreement and the terms of this DPA, the relevant terms of this DPA shall prevail, by way of exception to Section 1.3 of the Cloud Service Agreement.

1. DEFINITIONS

1.1 All capitalized terms not defined herein shall have the meanings set forth in the Cloud Service Agreement.

[Note: for additional definitions, as applicable according to the applicable Data Protection Legislation and Regulations, see the example below]

For the purposes of this DPA,

"Controller" means the Adopter;

"Model Clauses" means the standard contractual clauses annexed to EU Commission Decision 2010/87/EU of 5 February 2010 for the Transfer of Personal Data to Processors established in Third Countries under Directive 95/46/EC of the European Parliament and of the Council of October 24, 1995, as amended, on the protection of individuals with regard to the Processing of Personal Data and on the free movement of such data;

"Processor" means the Provider.

2. DESIGNATION OF PROVIDER AS PROCESSOR

2.1 By signing the Cloud Service Agreement the Adopter designates the Provider as Data Processor with regard to the Adopter's Personal Data within the scope of the Cloud Service Agreement as specified under Section 2.1 of the Cloud Service Agreement, and the Provider agrees to act as Data Processor in accordance with the terms of the Cloud Service Agreement and this DPA.

2.2 If the Processor is based outside the European Union, in a country that has not been subject to an adequacy (or equivalent) finding by the European Commission, its Personal Data Processing shall also be governed by the terms of the Model Clauses [Note: Model Clauses to be attached to this DPA as an Addendum] and this Data Processing Attachment applies insofar as it does not contradict the Model Clauses.

3. DURATION

3.1 This DPA shall be effective as from the Effective Date, and shall remain in force for the entire duration of the Agreement unless terminated in advance on any ground.

3.2 Upon termination of this DPA, the Provider shall return or otherwise make available for retrieval the Personal Data, or destroy all Personal Data (and certify that such Personal Data has been destroyed on the Systems and all storage media, including media of any Subcontractors) as specified under Section 10 of the Cloud Service Agreement, except as

[75] See note no.2.

otherwise required by the applicable Data Protection Legislation and Regulations.

4. TYPES AND CATEGORIES OF PERSONAL DATA AND PURPOSES OF PROCESSING

4.1 In order to execute the Cloud Service Agreement and to perform the Services on behalf of the Adopter, the Controller authorizes and requests the Processor to Process the following Personal Data:

a) Categories of Personal Data: Personal Data may include, among other information, [Note: list of Personal Data that may be Processed by the Provider under the Cloud Service Agreement depending on the services carried out by the Provider, e.g. personal contact information such as name, home address, home telephone or mobile number, fax number, email address, and passwords, financial details, etc.];

b) Categories of Data Subjects: Data Subjects include [Note: list of Data Subjects to whom Personal Data relate depending on the services carried out by the Provider, e.g. the Adopter, in case of a consumer using the Provider's Services; Adopter's employees, job applicants, contractors, customers, end users, Third-Parties, injured parties, etc.].

4.2 The Provider shall Process Personal Data solely for the purpose of the provision of the Services under the Cloud Service Agreement as described in details in Attachment 1 to the Cloud Service Agreement.

5. ADOPTER'S RESPONSIBILITY

5.1 The Adopter, as Controller of the Personal Data, is fully responsible for abiding by Data Protection Laws and Regulations and for compliance with its obligations, including providing legal basis for the Adopter's and Provider's lawful Processing of Personal Data under the Cloud Service Agreement, e.g. filing any required notifications or authorization, providing notices to and obtaining consent (as applicable) from the Data Subject.

6. ADOPTER'S INSTRUCTIONS

6.1 If necessary to comply with the Data Protection Laws and Regulations, during the term of the Services the Adopter may provide instructions to the Provider in addition to those specified in the Cloud Service Agreement.

6.2 The Provider will comply with all instructions provided by the Adopter without additional charge to the extent necessary for the Provider to comply with laws applicable to its performance of the Services as Data Processor.

6.3 The Provider will inform the Adopter if, in the Provider's opinion and without any obligation to perform any legal assessment, an instruction breaches Data Protection Laws and Regulations.

6.4 The Adopter and the Data Processor will negotiate in good faith with respect to any other change in the Services and/or fees resulting from such instructions.

7. PROVIDER'S OBLIGATIONS

7.1 The Provider shall not Process or use Personal Data for purposes other than those set forth in the Cloud Service Agreement or as instructed by the Adopter and shall not

disclose, or otherwise share the Personal Data with Third-Parties other than its Subcontractors for the aforementioned purposes or as required by European Union or EU Member State law to which the Processor is subject.

7.2 If the Processor is required by European Union or EU Member State law to process or disclose Personal Data for purposes other than set forth in the Cloud Service Agreement, the Provider shall promptly inform the Adopter of that legal requirement before Processing the Personal Data, unless that law prohibits such information on important grounds of public interest (e.g. secrecy duties related to criminal investigations).

7.3 The Provider will ensure that access to Personal Data will be limited solely to those of its staff, employees and representatives, under strict confidentiality provisions, who require access to the Personal Data as necessary for the provision of the Services and suitably trained in the Processing of Personal Data and in the technical and organizational security measures to apply.

7.4 The Personal Data will be erased from the System and any storage media no later than [●] days after the termination of any retention period specifically agreed with the Adopter and in any case upon deletion of the Personal Data by the Adopter. The erasure will be carried out according to the procedure defined under Section 10 of the Cloud Service Agreement or any alternative procedure mutually agreed in writing by the parties.

7.5 The Provider will promptly inform the Adopter of any demand from an executive or administrative agency or other governmental authority that it receives and relates to the Personal Data under the Cloud Service Agreement. At request of the Adopter, the Provider will provide the Adopter with reasonable information required for the response to the demand and any assistance reasonably required for the Adopter to respond to the demand in a timely manner, being excluded any responsibility of the Processor to liaise directly with the relevant authority unless otherwise required under the applicable Data Protection Laws and Regulations.

7.6 In addition, the Processor will provide reasonable cooperation to the Adopter, at the Adopter's reasonable request and within the timescales reasonably specified by the Controller, to provide all information, at its hand and strictly relevant to the Services, necessary to the Adopter (i) to make the processing notification with the competent data protection authority, (ii) to comply with any authorization or privacy assessment procedure to comply with the Data Protection Laws and Regulations, (iii) to allow the Adopter to comply with the rights of Data Subjects, including subject-access rights, or with notices served by any law enforcement authority and (iv) to demonstrate compliance with the Adopter's obligations under the Data Protection Laws and Regulations.

8. SUBCONTRACTING

8.1 In the event of any subcontracting enlisted by the Provider in accordance with the relevant provision of the Cloud Service Agreement of any Processing operations of the Personal Data, the Provider will timely inform the Adopter of any intended subcontracting and of the Processing operations to be enlisted to the Subcontractor.

8.2 The Adopter will retain the right to object to the subcontracting and it may withhold its consent, within a period of [●] days from the date of receipt of the notice, or terminate the Cloud Service Agreement with a [●] [days] written notice only on the basis of

reasonable grounds, including any restriction prescribed under the Data Protection Laws and Regulations.

8.3 [Note: to be included, as applicable] A list of Subcontractors as of the Effective Date is provided in Annex [●] to this DPA and, by signing the Cloud Service Agreement, the Adopter approves this list. Any addition or replacement to this list will be notified by the Provider to the Adopter via email to the contact addresses identified under the Cloud Service Agreement or via any other electronic form capable of being evidentiary documentation. The Adopter will retain the right to object to the intended changes and it may withhold its consent, within a period of [●] days from the date of receipt of the notice, or terminate the Cloud Service Agreement by written notice after [●] [days] written notice only on the basis of reasonable grounds, including any restriction prescribed under the Data Protection Laws and Regulations.]

8.4 The Adopter may request the Provider (i) to provide the Adopter with copies of the relevant terms of subcontracting agreement with Subcontractors (with omission of any confidential information, if any) and (ii) to audit, at least once per year, the Subcontractors in relation to their compliance with the security measures and the Processing of Personal Data in accordance with the instructions of the Adopter under Section 6 to this DPA, or confirm that such an audit has occurred (or, where available, obtain or assist the Adopter in obtaining a Third-Party audit report concerning the Subcontractor's operations), providing a copy of such report according to Section 12 below.

8.5 Where the Provider engages any Subcontractor for the processing of Personal Data, the Provider will ensure that the subcontracting agreement includes (i) an explicit designation – in the name, and on behalf, of the Adopter – of the Subcontractor as Adopter's Data Processor or any other legal act valid under the European Union or the EU Member State law, (ii) obligations upon the Subcontractors in relation to the Processing of Personal Data, including implementation of security measures, at least equivalent to those set forth under the Cloud Service Agreement (especially, but not limited to those set forth under Attachment 6) and (iii) the Subcontractors' liability towards the Provider and the Adopter.

8.6 Where any of the Subcontractors fails to fulfil its data protection obligations, the Provider shall remain fully liable to the Adopter for the performance of that Subcontractor's obligations.

9. TRANSFER OF DATA

9.1 The Provider declares and warrants that for the provision of the Services it will use exclusively data centres located within the EU.

[Note: if transfer outside the EU is permitted by the Adopter, Section 9.1 will be the following:

The Provider represents, and the Adopter agrees, that Personal Data will be stored in the data centres located outside the EU [Note: listed below/under Annex [●] to this DPA/available at [●]].

9.2 Any addition or replacement to this list will be notified by the Provider to the Adopter via email to the contact addresses identified under the Cloud Service Agreement. The

Adopter will retain the right to object to the intended changes and it may withhold its consent, within a period of [●] days from the date of receipt of the notice, or terminate the Cloud Service Agreement by written notice after [●] [days] written notice only on the basis of reasonable grounds, including any restriction prescribed under the Data Protection Laws and Regulations.

9.3 [Note: if transfer outside the EU is permitted by the Adopter, the following clause should also be included: The Provider represents and warrants that [Note: insert details of the guarantees implemented by the Provider to ensure the transfer of Personal Data outside the EEA or the countries that have been subject to an adequacy (or equivalent) finding by the European Commission pursuant to Articles 25 and 26 of the Directive ("adequacy finding"), offer equivalent protection to the data. Please refer to any documentation attached to the Cloud Service Agreement specifying whether the transfer is based on (i) Binding Corporate Rules , (ii) on Model Clauses or (iii) on any other adequacy ground approved by the EU Commission, e.g. the EU-US Privacy Shield[76]].

9.3 [Note: if transfer outside the EU is permitted by the Adopter, the following clause should also be included: If the Adopter approves any subcontracting outside the EEA in a country that does not offer an adequate protection of Personal Data as provided under the Directive 95/46/EC[77], the Adopter hereby expressly mandates the Provider to enter– in the name, and on behalf, of the Adopter –into the Model Clauses whose Annex 1 and Annex 2 shall be substantially in line with the information under this DPA and to provide, at request of the Adopter, copy of the signed Model Clauses.

10. RIGHTS OF THE DATA SUBJECTS

10.1 To the extent legally permitted, the Provider agrees to promptly notify the Adopter if it receives any requests, notices or other communication from Data Subjects for the Adopter for access to, correction, amendment, blocking, deletion of that Data Subject's Personal Data or objection to the Processing Personal Data of that Data Subject.

10.2 Upon written request of the Adopter [and at no additional cost/ upon payment of reasonable fees associated with the performance of any such operation], the Adopter will be granted electronic access to the Adopter's Service environment that holds Personal Data to permit the Adopter to extract, access, correct, amend, block access or delete specific Personal Data. If that is not practicable and to the extent permitted by Data Protection Laws and Regulations, the Provider will perform such operations upon the Adopter's detailed written instructions.

10.3 The Provider shall not respond to any such Data Subjects' request without the Adopter's prior written consent.

11. SECURITY

11.1 When Processing Personal Data on behalf of the Adopter in connection with the provision

[76] Adequacy of the measures set forth under the former US-EU Safe Harbor has been challenged by the Court of Justice of the European Union (*Maximillian Schrems v. Data Protection Commissioner (Safe harbor – Case C-362/14*) ruling that the US-EU Safe Harbor data transfer agreement is invalid. A new EU-US Privacy Shield has been negotiated at political level between the EU Commission and the U.S. Department of Commerce on February 2nd, 2016; formal approval of the Umbrella Agreement is expected during 2016.

[77] See note no.2.

of the Services, the Provider will cooperate with the Adopter to have in place appropriate physical, technical and organizational security measures for the Processing of such data in compliance with the security requirements set forth under the applicable law, including Data Protection Laws and Regulations, as applicable, to protect Adopter Personal Data against accidental or unauthorized loss, destruction, alteration, disclosure or access, and against all other unlawful forms of processing.

11.2 Among others, the Provider agrees to maintain for the entire Duration of the Cloud Service Agreement, the physical, organizational and technical security measures specified in Attachment 6 to the Cloud Service Agreement to ensure the availability, integrity and confidentiality of the Personal Data, including monitoring use of the System by any "administrator".

11.3 The Provider will not materially decrease the overall security of the Services during the term of the Cloud Service Agreement.

11.4 In the event that the Provider becomes aware of any confirmed or suspected security breaches or breaches of any provision of the DPA and/or any irregularity in the processing of the Personal Data, or in the event that the Provider is contacted by a supervisory authority for data protection violation, the Provider will promptly notify the Adopter. in the event of a security breach triggering notification obligations for the Adopter under applicable Data Protection Laws and Regulations, the Provider shall cooperate with the Adopter to identify and remediate the cause of such breach. The Provider will maintain security incident management policies and procedures as described in Attachment 6 (as amended from time to time, provided that the overall efficacy of the procedure will not decrease).

12. REPORTING AND AUDIT

12.1 On an annual basis (starting from the end of the first annual year of duration of the Cloud Service Agreement) and occasionally, upon a reasonable and motivated request of the Adopter, the Provider will monitor its compliance with its data protection obligations in connection with the Services provided to the Adopter and will provide the Adopter with a written report on the results of such controls.

12.2 [Note: if applicable] The Provider has obtained the third-party certifications and/or audits set forth in Attachment 6 to the Cloud Service Agreement. Upon the Adopter's written request at reasonable intervals (i.e. once per year or earlier if grounded on valid legal reasons) the Provider will provide a copy of the Provider's then most recent third-party certifications and/or audits, as applicable, or any summaries thereof, as generally made available to its customers at the time of such request.

12.3 The Adopter may audit, at its expenses, the Provider's compliance with the terms of the Cloud Service Agreement and this DPA up to once per year. The Data Controller may perform more frequent audits of the Systems that Process Personal Data to the extent required by laws applicable to Data Controller or, at the Provider's expenses, based on a valid reason (e.g. actual or reasonably suspected unauthorized disclosure of Personal Data). If the audit is to be conducted by a Third-Party, the Adopter and the Provider will identify, by mutual agreement, this Third-Party. The Third-Party will sign a written confidentiality agreement before conducting the audit.

12.4 Any request of audit is submitted with appropriate notice (at least [●] weeks in advance

of the audit). *12.5 The audit will be conducted during regular business hours at the applicable facility, subject to the Provider's policies and may not unreasonably interfere with its business activities.* *12.6 A copy of the audit report will be provided by the Adopter to the Provider, unless prohibited by law. The Provider will submit to the Adopter an action plan to remedy any non-conformity identified during the audit and will put in place adequate measures to remedy within the timescale agreed with the Adopter.* *12.7 Audit reports can only be used by the Parties to achieve their regulatory requirements and/or confirming compliance with the requirements of the Cloud Service Agreement.* *13. GOVERNING LAW* *13.1 This DPA shall be governed by, and construed in accordance with, the Data Protection Laws and Regulations of [country of establishment of the Adopter].*

Attachment 6 to the Agreement: Security Policy

Description of the SLALOM Attachment
This policy concerns the responsibilities of the Parties in relation to security measures to be implemented by the Provider. Security measures must be outlined in the document and must be aligned at least with suitable set of physical, technical and organizational measures as set out by the applicable Data Protection Laws and Regulations.
SLALOM Introduction of this Attachment
The Provider shall implement and maintain the following security measures in the provision and the use of the Services.

Document contributors

Gian Marco Rinaldi (Bird & Bird)
Debora Stella (Bird & Bird)
Roger Bickerstaff (Bird & Bird)
Barry I Jennings (Bird & Bird)
Alexander Duisberg (Bird & Bird)
Stephane Leriche (Bird & Bird)
Leonidas Kanellos (UPRC)
Aimilia Bantouna (UPRC)
Panagiotis Vlaheas (UPRC)
Andreas Georgakopoulos (UPRC)
Konstantinos Tsagkaris (UPRC)
Panagiotis Demestichas (UPRC)
Mavreta Stamati(UPRC)

REFERENCES

[1] SLALOM D3.1 Initial Position Paper (Technical)
[2] SLALOM D3.2 SLA Specification and reference model a
[3] SLALOM D4.1/5.1 Initial Position Paper (Provider and Adopter's perspectives)
[4] SLALOM website: www.slalom-project.eu