CLOUD
ACCOUNTABILITY
PROJECT

D: D-4.3 Guidelines and tools for cloud contracts

Deliverable Number	D44.3
Work Package	WP 44
Version	Final
Deliverable Lead Organisation	TiU
Dissemination Level	PU
Contractual Date of Delivery (release)	30/09/2015
Date of Delivery	30/09/2015

Editor

Dimitra Stefanatou (TiU)

Contributors

Rehab Alnemr (HP), Lorenzo Dalla Corte (TiU), Brian Dziminski (QMUL), Niamh Gleeson (QMUL), Amy Holcroft (HP), Eleni Kosta (TiU), Ronald Leenes (TiU), Rodney Mhungu (TiU), Siani Pearson (HP), Chris Reed (QMUL), Adele Calamo Specchia (TiU), Kees Stuurman (TiU), Dimitra Stefanatou (TiU)

Reviewers

Jesus Luna (CSA), Christoph Reich (HFU)

A4Cloud
www.a4cloud.eu
Accountability For Cloud and Other Future Internet Services
FP7-ICT-2011-8-317550-A4CLOUD

SEVENTH FRAMEWORK
PROGRAMME

Executive Summary

This deliverable builds upon the findings of an earlier survey conducted by the project on standard cloud contracts and Service Level Agreements (SLAs)[1].This research provided an overview of the state of the art and best practices on how exactly to strengthen accountability though contractual agreements. Second, it provided input to the development of the Cloud Offerings Advisory Tool (COAT) by pointing out which clauses of cloud contracts covering data protection related issues to compare. Third, it gave insights to further research – still ongoing within the project at the time of writing this deliverable – concerning the assessment of maturity level of organizations with respect to accountability. The latter is being partly addressed here, given that it forms work in progress.

This deliverable sets the scene of the cloud computing market, explaining the weak position for end users and Small and Medium Enterprises (SMEs) when deciding which cloud offer suits them best. A primary reason of the weak position of SME's is their lack of resources and expertise compared to large organizations, hence it is hard for them to make informed choices regarding services from the viewpoint of personal data protection. There is a lack of transparency regarding the features of the different offerings, hampering SME's making informed choices regarding appropriate cloud offerings. The reasons for this lack of transparency range from the jungle of documents forming the vast majority of standard cloud contracts to the complexities posed by cloud computing technology per se.

A cloud contract – as is the case for contracts in general – is any legally binding agreement, which is formed though an offer and an acceptance between two or more consenting parties. Cloud contracts can be grouped into two categories: standard non-negotiated contracts and negotiated contracts. Standard contracts are agreements, which are compiled of standardized non-negotiated terms. They are used in business to consumer models and business-to-business models where mass services are distributed, because they provide efficiency in not having to spend time and money in negotiating specific details. Negotiated contracts are agreements between parties who have more symmetry of bargaining power between them than those described in standard form contracts. Here, the parties will both be given the opportunity to put forward their own terms and request changes to any standard terms presented by the other party. Such contracts are less common, at least numerically, in cloud transactions, though almost all high value contracts will be negotiated. Taking into account, however, that negotiated contracts are not available on line, and that cloud end users hardly have any power to negotiate a contract with cloud service providers (CSPs), this deliverable essentially expands on standard contracts.

Given the increasing number of CSPs offering often their services for free, cloud end users and SMEs are confronted with a plethora of choices, which complicates decision making. The existence of choice allows for comparisons as a means to support decision making, rendering the final decision potentially more beneficial for the users of cloud services. To draw lessons from other domains where users are confronted with multiple dimensions on which to compare service offerings, this deliverable gives an overview of the regulatory framework governing existing online comparison websites for utility services and insurance. The comparison websites in these two domains provide inspiration for the Cloud Offerings Advisory Tool (COAT) developed in this work package. Also, drawing links with how comparison websites work is highly relevant for the present analysis due to the fact that COAT basically functions as a cloud broker/matchmaking component focusing on traits relevant to accountability.

COAT is part of the A4Cloud toolbox providing information/advice before making a decision, therefore, functioning as a preventive accountability mechanism. It fosters CSP's being transparent (and through committal in the tool, to accountability) about their offerings; also, it assists cloud customers (SMEs) in choosing a cloud service tailored to their needs by probing user needs through a set of questions and attribute selections, by matching those answers to characteristics of concrete cloud offerings and by listing matching offerings.

[1] Reed, Chris et al., "*Report of survey of cloud contract terms*", Cloud Accountability Project D: D-4.2, Gleeson et al. (eds.), 2015.

COAT's questionnaire is based on research of contract terms used in standard cloud contracts, relevant provisions in the data protection legal framework (both Data Protection Directive, and proposed General Data Protection Regulation). This level of regulation is chosen because, despite the variations at national level, the general rules and principles of data protection law within EU are general. Central in COAT's functioning are the characteristics of cloud offerings, known as “attributes”. By attributes, under this deliverable, we mainly refer to those traits of cloud offered services covered by cloud contracts and service level agreements that would be meaningful to compare bearing in mind the project's scope and the aims of the tool. A dynamic filtering process matches the attribute-value pairs selected by the user with those of cloud offerings and presents matches to the user. The tool provides explanation about the attributes and their values to help the user asses in a simplified manner complex legal terms. Specific issues like Intellectual Property Rights (IPRs) that hardly varied across Software as a Service (SaaS) contracts or technical questions that would require extended technical knowledge were, therefore, left out from COAT's questionnaire.

This document explains in detail the reasoning behind the COAT tool as well as on the potential benefits for cloud customers (SMES). Given that the number of CSPs grows and, therefore, the chances that the offers suggested, also, rise, the listing of the offers at the end of the selection process becomes increasingly important. Therefore, what is currently being investigated by the project is whether the accountability maturity level of a CSP could be the determining factor for the listing of the proposed CSPs by COAT.

Finally, the deliverable concludes with concrete suggestions for best practices on how CSPs could best promote accountability from a data protection viewpoint through standard contracts, as well as with a summary of potential benefits resulting from COAT.

Table of Contents

1 Introduction

This section gives an overview of certain current issues regarding cloud contracts from the viewpoint of cloud customers (end users and SMEs) highlighting their impact on the enforcement of accountability within cloud ecosystems. Note that Building on this problem statement, the discussion below draws links between the research presented in this document and its relevance with the project's scope. Finally, the section sets the outline of the analysis to follow.

1.1 Setting the scene for contracts and cloud contracts

Contracts

A contract can be defined as any legally binding agreement. The agreement gives rise to obligations to perform the promises made to the other party or parties to the contract, which are enforced and/or recognized by the law. The agreement is formed through an offer and acceptance between two or more consenting parties.

It is important to note that, in general, a contract does not need to be set down in writing. Agreements are made verbally, or even through conduct, every day. If those agreements meet the requirements set in the context of each jurisdiction, which make them legally binding, they are contracts. Contracts specify what it is provided by national laws and/or provide, of course, for aspects not covered by the regulator. In any event, contracts cannot provide against what it stipulated by law (e.g. European Directives, national implementing laws)[2].

Both within common law (e.g. UK, USA) and civil law jurisdictions (e.g. France, Germany) a valid contract requires an offer and an acceptance. An offer is a set of terms under which the offeror (the party making the offer) is willing to be bound. An offer is made to the offeree (the recipient of the offer) and he/she must accept in the method expressed (if stipulated) by the offeror. Moreover, acceptance implies that the offeree must accept the terms of the offer. This means outward evidence of the offeree’s intention to accept an offer has to be demonstrated (in unilateral and bilateral contracts) and communicated (in bilateral contracts) in order for effective acceptance; mere silence is not effective acceptance.

Despite the commonalities, in general, between common law and civil law traditions, there are also significant differences. Under the common law tradition “consideration” is also required for a contract to be valid. Consideration in contract law is merely something of value that is provided and which acts as the inducement to enter into the agreement. It must amount to a benefit for the promisor, or a detriment (some kind of cost, though not necessarily in money) to the promisee. This consideration is, in effect, the payment for the promisor’s promise. Consideration need not be in money terms - the promisee may exchange promises with the promisor, or he/she may provide some act or forbearance to establish good consideration, for example payment for the service or product. By contrast, the contracts in the civil law countries are enforced on the consent of the parties. One limit to the validity of contracts is the possible lack of a “positive social function” or being contra bonos mores. Furthermore, the civil code of each country sets out the particular requirements for a contract to be valid that may, nevertheless, vary between different jurisdictions. The analysis shows that these differences between different legal systems, essentially, emerge in cloud contracts as well. As it will be pointed out later in the text, certain areas in which these legal systems differentiate will be discussed further under “D-4.4 Remediation guidelines and tools’’[3].

Cloud contracts

[2] For example, European Commission (EC) (1995) ‘Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data’, as implemented by the UK’s Data Protection Act 1998.

[3] This deliverable will be produced under “T:D-4.3 Development of mechanisms and tools for redress’’, due in December 2015.

A4Cloud project has identified contracts as a privileged accountability delivery mechanism for the stewardship of personal information in the cloud[4].

In particular, contracts could be an effective mechanism to impose accountability obligations and to clarify how service providers and users will meet the accountability obligations from external regulation (e.g. EU laws, national legislation). It is clear, though, that the terms offered in the majority of cloud agreements are not completely effective in enforcing accountability obligations in practice. Although the obligations in most relationships are identified, cloud contracts are not drafted in such a way that would enhance transparency of processing operations in the cloud allowing for educated choices by all users of cloud services.

The main issue, which has affected the role of contracts, is that cloud agreements do not clearly identify and understand what these specific obligations should actually be. The reasons for this are complex: there are no standard terms (except those implied by law) in standardized contracts, the cloud market is still developing and several large cloud providers currently dominate it. Standard terms in cloud agreements have been mostly dictated by such providers, but these standard terms differ, while negotiated contracts are only available in limited situations. In addition, it is considered that “accountability and responsibility are seemingly fading or disappearing’’[5] in the cloud due to the chain of sub-contractors. The result being accountability is reduced in its value to impose responsibilities and obligations on the correct actors in the cloud agreement.

Most importantly, the role of contracts in ensuring accountability is very much influenced by the negotiating power of the parties. The substantial imbalance of powers between the cloud service providers and the cloud customer (end user or SME) creates an impact on the accountability obligations, which can be reflected through contractual clauses. Many cloud agreements are standard form since cloud computing is most commonly the offering of services based on a one-to-many model. Many cloud providers have adopted click wrap agreements, which are a type of standard form contract associated with software licensing. In practice, "click wrap agreements" involve the end users indicating consent or rejection to the provider’s terms and conditions on their screen. Usually the terms will be on a separate page which is linked to the actual acceptance screen.

As opposed to standardized contracts, negotiated contracts are between parties who have more symmetry of bargaining power between them than those described in standard form contracts. Here, the parties will both be given the opportunity to put forward their own terms and request changes to any standard terms presented by the other party. Such contracts are less common, at least numerically, in cloud transactions, though almost all high value contracts will be negotiated.

1.2 The "less empowered" players: end users and SMEs

Given the imbalance of power in the cloud computing market, also, reflected by the widespread use of standardized contracts, the research captured in this Deliverable, concentrated on investigating the needs of individual end users and SMEs[6]. According to several sources[7], end users and SMEs constitute the less empowered players within the cloud computing market, which explains why aiming at assisting them decide which cloud service suits them best.

This imbalance results both from the luck of equally distributed negotiating power as well as from the luck of resources and expertise. As opposed to large corporations that have adequate resources to include in their structures separate departments (e.g. Legal or IT departments), cloud end users and

[4] D:B-5.1 White paper on the proposed data protection regulation, available at http://www.a4cloud.eu/sites/default/files/D25.1%20White%20paper%20on%20new%20Data%20Protection%20Framework.pdf

[5] Working Paper on Cloud Computing-Privacy and data protection issues- “Sopot Memorandum” adopted by the International Working Group on Data Protection in Telecommunications on the 24th of April 2012, page 2.

[6] This is clearly reflected in the selection of attributes for the creation of COAT questionnaire discussed later under section 5.

[7] Opinion of the European Data Protection Supervisor on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe", 16th November 2012, para.21.

SMEs are expected to make a decision on which cloud offering suits them best without necessarily having any particular knowledge or expertise.

As with any commercial agreement, the bargaining power of the parties will dictate -to some extent- the possibility of negotiations and how fruitful they are. One can perceive this to be the reason why the majority of cloud agreements, which offer consumer products, are click wrap agreements. The cloud provider will be offering the service on the one-to-many model – if the user is not happy with certain terms it must seek another provider, as these terms are not negotiable. In contrast, where the user is seen to be of value or high net worth, such as large international organizations (for example financial institutions) or large government entities, then providers are more likely to agree to negotiations, even if this is only with respect to commercial terms.

Interestingly, this imbalance of power does occur -from a different viewpoint- in between individual end users and SMEs. While this distinction is of minor significance when dealing with the data protection issues arising from cloud contracts, the protection available for a contracting party depends, also, on its qualification as a natural person/consumer[8] or a legal entity/company. Individual end users of cloud offered services are, therefore, protected on the basis of consumer protection law. Concerns regarding comparison websites from the view point of consumer protection will be addressed under section 4 of this deliverable.

1.3 Aims of the deliverable

This deliverable forms the public output of the research conducted within "T: D-4.4 Guidelines and tools for cloud contracts". The deliverable builds on the research findings produced under "T: D-4.2 Survey of evolving contract terms and SLAs''.

In particular, the deliverable builds on the state of the art regarding cloud contracts in order to stress out certain issues that affect educated decision making. Having identified the complexities and taking into account the particularities for cloud end users and SMEs, the deliverable aims at addressing their needs by creating a tool, namely, the Cloud Offerings Advisory Tool (COAT), which facilitates them in choosing an appropriate cloud service.

Furthermore, the deliverable provides best practices for CSPs on how to promote accountability, especially, with respect to data protection issues through standardized contracts; in that sense, the research summarized in this document covers both sides of the spectrum, meaning the parties offering the cloud services (CSPs) and those using them (cloud customers).

1.4 Relevance with the project's scope

The research outputs described here link to the project's scope[9]: an accountability tool is built and the accountability framework is further expanded.

[8] The European Court of Justice, in the case Cape V. Ideal Service, clearly stated that "the term consumer, as defined in Article 2(b) of the Directive [93/13], must be interpreted as referring solely to natural persons."

[9] Dziminski et al., in the ''*Report detailing conceptual framework"* (Cloud Accountability Project, D:C-2.1, 2014) describes the project's scope as follows: "*The overall goal includes development of techniques that can enable improved trustworthiness of cloud service provision networks, and to prevent breaches of trust by using audited policy enforcement techniques, assessing the potential impact of policy violations, detecting violations, managing incidents and obtaining redress. The outputs of the project include an accountability framework (including recommendations, guidance, models of data governance, accountability metrics and a reference architecture) as well as a range of accountability tools and mechanisms. These are being developed for individuals and organisations using cloud services as well as for cloud service providers and regulators. The focus of the project is on personal data, but in addition certain types of confidential information that may not involve personal data, such as business secrets, are being considered. The focus is particularly on the accountability of organisations using and providing cloud services to data subjects and regulators*".

In particular, COAT is part of the project's toolset providing for information/advice[10] helping cloud customers to choose a cloud service in an intelligible way, based on their data protection and security requirements. COAT focuses on those contract terms that link to data protection in the cloud. Given that issues of business confidentiality would be relevant only for a part of the potential users of COAT and the absence of such terms in publicly available standard contracts, this sort of considerations linking to business confidentiality obligations are, essentially, left out from this discussion.

Moreover, the present analysis strengthens the accountability framework built by the project in two ways: first, it provides guidance by proposing best practices on how CSPs could best promote accountability through contracts and second, it paves the ground for the production of metrics that would measuring the accountability maturity level of comparable organizations through COAT.

1.5 Outline of the deliverable

The deliverable is composed of six (6) sections, including, conclusions. A glossary of legal terms and a list of tables and figures are incorporated in the appendices. The appendices, also, include a report summarising the findings following a trial of an earlier version of COAT demo with potential users of the tool.

In particular, section 2 explains how exactly accountability and transparency relate to decision making; to this end, the section discusses in detail transparency issues of standard cloud contracts and how they hinder making an informed choice. Section 3 introduces the concrete findings of the earlier stated survey conducted on standard contracts; it incorporates examples of contract terms that are significant from the point of view of accountability as identified by the project. In view of the discussion to follow on COAT -and bearing in mind its function as a cloud broker- section 4 gives an overview of the regulatory framework governing comparison websites already available in the market covering different sectors, other than cloud services. Building on the previous analysis, section 5 describes then the functionalities of COAT, listing concrete inputs and outputs of the tool and reflecting on potential benefits. Moreover, section 5 reflects briefly on how a creation of an accountability maturity model could be relevant for ordering the proposed offers appearing at the end on user’s screen.

Finally, the last section of the deliverable summarizes the benefits of COAT tool, pointing out as well certain limitations. Section 6, also, incorporates recommendations addressed to CSPs on how to strengthen accountability through specific clauses included in standardized cloud contracts.

[10] Gleeson et al., "*A4Cloud Tool, Liability and Compliance Investigations",* Cloud Accountability Project D-4.12 Gleeson et al. (eds.), (2015).

2 The Concept of Accountability

This section expands on how accountability enables decision-making. It does so by pointing out the links between certain accountability attributes identified under WPC2 and how the Cloud Offerings Advisory Tool (COAT) works, which will be explained in detail later in the text. This section reflects on the actual circumstances, which would pave the ground for cloud subjects[11] to make an informed choice of the appropriate cloud service from the point of view of personal data protection.

2.1 Transparency as an accountability attribute for decision making

The project has identified a set of core accountability attributes, namely, transparency, responsiveness, remediability, responsibility, verifiability, effectiveness and appropriateness[12] several of which are clearly reflected in the way certain tools work. The remediability attribute, for instance, relates to the aims of the Redress & Remediation Tool (RRT) which aims at providing advice on how potentially to obtain redress; similarly, the Data Protection Impact Assessment Tool (DPIAT)[13] links to the attribute of verifiability. As it will be further explained below, though, the research captured in the present document primarily links to the transparency attribute.

According to the definitions adopted by the project, *"transparency is the property of a system, organisation or individual of providing visibility of its governing norms, behaviour and compliance of behaviour to the norms.*" This property is implemented through accountability mechanisms such as contracts. What is crucial but yet, however, fairly misunderstood in practice is that the notion of transparency is not exhausted in information giving acts or in the provisioning of large amounts of such information. On the contrary, it relates as well to whether the information given to the user is presented in an understandable manner; the latter appears to be exceptionally challenging in cloud environments due to the complexities posed by cloud computing technology itself.

From the point of view of personal data protection, it is argued that there are two main categories of risks concerning processing through the cloud[14]: a) the loss of control on the user's side and b) the absence of transparency regarding the circumstances under which the processing is performed. The absence of transparency in the cloud can be manifested in multiple ways such as the lack of information in relation to the chain of actors involved in the processing or the locations where processing is performed, including transfers outside the European Economic Area[15]. Moreover, the issue of transparency in the cloud and the extent to which it is ensured through contracts becomes even more complicated if we take into account the way they are publicly displayed. The potential user of a cloud service needs to navigate through a jungle of documents available online (e.g. Terms and Conditions, Privacy Policy, Intellectual Property Right etc.) in order to decide whether a particular cloud service suits

[11] A detailed description of all cloud roles can be found in Dziminski et al., ''*Report detailing conceptual framework",* Cloud Accountability Project, D:C-2.1, (2014).

[12] A detailed analysis of all the accountability attributes identified by the project can be found in Dziminski et al., ''*Report detailing conceptual framework",* Cloud Accountability Project, D:C-2.1, (2014).

[13] See, also, Gleeson et al., "*A4Cloud Tool, Liability and Compliance Investigations",* Cloud Accountability Project D-4.12 Gleeson et al. (eds.), (2015).

[14] Directorate General for Internal Policies Policy Department A: Economic And Scientific Policy, "*Cloud Computing – Study*", IP/A/IMCO/ST/2011-18 May 2012 PE 475.104 (2012).

[15] It is, therefore, recommended that controllers should also as a matter of good practice provide further information relating to the (sub-) processors providing the cloud services. As it is stated in this respect, "Transparency must also be ensured in the relationship(s) between cloud client, cloud provider and subcontractors (if any) (…) A controller contemplating engaging a cloud provider should carefully check the cloud provider's terms and conditions and assess them from a data protection point of view. Transparency in the cloud means it is necessary for the cloud client to be made aware of all subcontractors contributing to the provision of the respective cloud service as well as of the locations of all data centres personal data may be processed (…) If the provision of the service requires the installation of software on the cloud client's systems (e.g., browser plug-ins), the cloud provider should as a matter of good practice inform the client about this circumstance and in particular about its implications from a data protection and data security point of view. Vice versa, the cloud client should raise this matter ex ante, if it is not addressed sufficiently by the cloud provider." European Parliament Cloud Study available at: http://www.europarl.europa.eu/RegData/etudes/etudes/join/2012/475104/IPOL-IMCO_ET(2012)475104_EN.pdf

him or not.[16] Note that these documents are written in a language not easily understood by ordinary users with no relevant expertise. And if this skimming through the contract of one service is complicated, doing so several times to compare and finally decide is not that simple if it is about a decision to be made by an end user or an SME[17].

Furthermore, transparency implies a sort of balancing the information which can be given to the cloud customer -and, eventually, to the cloud subject- with the information that is appropriate to be given[18]. Article 29 Working Party points out in this respect: "*the client should be provided with meaningful information about technical and organisational measures implemented by the provider"*. The statement implies a sort of filtering of the information that should be given to the cloud client. The end user should not, therefore, be overloaded with the maximum information possible, but only with this sort and amount of information that would have an actual meaning. In this context, information that lacks clarity cannot be meaningful, in the sense that a certain purpose aspired (e.g. transparency regarding the supply chain) can be very well undermined due to inappropriate linguistic means employed.

2.2 Cloud contracts as a tool for decision making

Given the fluidity and the complexity of the cloud computing environment, the role of contracts is very important, also, with respect to legal certainty and how it potentially affects making a decision with respect to a particular cloud offering. For instance, certain clauses might be drafted in a way to increase providers' flexibility, while at the same time reducing users' certainty towards the service's characteristics (e.g. clauses allowing unilateral changes by the service provider). Nevertheless, the overall content of a cloud contract entails a decision to accept or not accept the terms regarding the offer of a certain service and, therefore, should provide the right information in an appropriate manner to enable well informed decision making.

Article 29 Data Protection Working Party (A29WP) has provided in this respect a set of recommendations regarding specific issues that should be put forward by cloud computing contracts[19]. In particular, it examines legal certainty in relation to the contractual safeguards of the controller–processor relationship. In this context, a cloud contract should stipulate that the processor must act under the instructions of the controller and that the processor must take security measures for the effective personal data protection. A29WP views these as the minimum requirements and recommends the inclusion of a number of additional terms to provide greater transparency and control for the user. These include providing details of the to the exact processing locations of data, the naming and prior approval of all sub-contractors and requirements in relation to the returning or destroying personal information.

Nevertheless, a well-educated decision regarding the acceptance or not of a cloud offering would most probably, also, result from a stage of negotiations between the parties, before the actual enforcement of the contract. This, however, is unfeasible when concluding an online cloud contact; standard cloud contracts are, basically, click-wrap mechanisms, which are quickly and easily set up and agreed upon. Moreover, the cloud environment is by definition rapidly scalable and characterized by an on-demand, pay-as-you-go model whose flexibility might cause the agreement to be perceived as not worth the same level of legal analysis that, for instance, a traditional IT outsourcing agreement would demand[20]: *"(t)he*

[16] The European Parliament considers the lack of transparency and the difficulties in finding information as two separate issues that create an impact for rights and responsibilities in the cloud: *"Rights and responsibilities in the cloud are not yet clear due to lack of transparency or difficulties in finding information, problems with contracts, the complexities of many jurisdictions or the fact that for each legal issue - data protection, contracts, consumer protection or criminal law - the jurisdiction may differ. There also gaps in the relevant legislation when applied to cloud computing*" http://www.europarl.europa.eu/RegData/etudes/etudes/join/2012/475104/IPOL-IMCO_ET(2012)475104_EN.pdf

[17] Note that the explicit request to agree with the Term and Conditions by ticking a box is what actually renders these documents contractual click through agreements.

[18] See footnote 11.

[19]Opinion 05/2012 on Cloud Computing by the Article 29 Working Party, adopted on the 1st of July 2012, pages 12-14.

[20] See Bradshaw, Simon, Christopher Millard, and Ian Walden. "*The Terms They Are A-Changin"… Watching Cloud Contracts Take Shape*", Issues in technology Innovation 7 (2011): 4.

inherent risk of this is that just because an agreement is seen as quick and relatively cheap to enter into it might also be seen as not being worth subjecting to proper legal scrutiny, especially if it is offered on standard terms rather than via a mutually-developed contract[21]". So, in this context, given the absence of any room for negotiation[22] for the cloud end users and SMEs and the fluidity of cloud offered services, it is questionable whether cloud contracts offered to end users and SMEs work actually as a mechanism for responsible decision making.

To promote transparency of cloud offering and stimulate cloud costumers to familiarize themselves with technical terms and, eventually, help them to make a more informed choice, we will proceed in decomposing the Terms of Service into their constituent components and have all customers go through them. The analysis below looks into the state of the art of standard cloud contracts and proposes a technical solution to mitigate the reasons hindering well informed decision making.

[21] Ibid.

[22] It is argued that: ''ttransparency towards the users and data subjects should be a fundamental objective of any cloud computing system'' Poullet, Yves, et al. "Cloud Computing and its implications on data protection." Council of Europe (2010), s. 7.'Taking this into account, transparency should not be an obligation of CSPs addressed only towards customers buying cloud offered services, but also towards customers using cloud services offered them for free.

3 Analysis of typical terms in contract terms & SLAs

This section builds on a prior analysis conducted by the project assessing – from an accountability view point – the state of the art and the trends developed with respect to standardized cloud contracts and service level agreements (SLAs).[23] Given that the vast majority of cloud service providers are located within USA, the legal analysis is made under the common law perspective, which is especially relevant with respect to how liability is conceived; references to civil law will be made, though, when necessary. The section explains in plain language the contract terms discussed mapping them with the accountability attributes identified by the project[24]. Note that the discussion included under this section, as well as, the Data Protection Directive (DPD)[25] and the proposed Data Protection Regulation (GPDR)[26] provided the basis for the selection of COAT attributes to be discussed later under section 5.

3.1 Selecting the 20 contract terms in a typical cloud contract

This section examines in detail the 20 most typical contract terms found in cloud standard contracts surveyed. Our methodology for identifying the 20 most typical contract terms in cloud contract relies on a series of surveys carried out between 2010 and 2015. The Cloud Legal Team in Queen Mary University of London in 2010 carried out a survey that identified 20 contract terms that most frequently occurred in standard contract offered by cloud providers.[27] A further survey was carried out in 2013 with the aim of comparing the 2010 results and the 2013 results and identifying changes in the contract terms of individual providers.[28] This time the survey extended to nearly 40 cloud standard contracts. Nevertheless, the standard 2O contract terms remained the same. Finally, as part of the A4Cloud project under T:D4.2 "Survey of evolving contract terms and SLAs" a further survey of cloud standard contracts has been conducted in 2015.[29]The same 20 contract terms featured in the contracts surveyed in 2015. For this reason, these are the contract terms that will be used for our analysis in this Deliverable.

The 20 typical contract terms are listed in the table below.

[23] Contracts or terms of service are used to refer to a set of documents containing the terms of the relationship between the customer and the cloud service provider. These documents range in complexity from a single document, called terms of service (ToS) to a collection of additional documents relevant to the relationship between the cloud service provider and the customer including Privacy Policies, Acceptable Use Policies and Service Level Agreements (SLAs). For the purposes of this document, when we refer to contracts or terms of service we include the additional documents. This is consistent with the surveys on cloud contracts conducted in 2010 and 2013, Bradshaw, Millard and Walden 'Standard Contracts for Cloud Services' in Millard (ed.) Cloud Computing Law (2013) 43-44 and the work done for the survey in 2015 as part of the Deliverable for A4Cloud D4.2 although that Deliverable also included a separate analysis of SLAs.

[24] Dziminski et al., ''*Report detailing conceptual framework",* Cloud Accountability Project, D:C-2.1, (2014).

[25] European Commission (EC) (1995) 'Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data', available at http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf

[26] European Commission, "Proposal for a Regulation of the European Parliament and of The Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)" COM 2012 (011) final

[27] Bradshaw S, Millard C and Walden I in 'Standard Contracts for Cloud Services' in Millard (ed.), Cloud Computing Law (2013, OUP Oxford), 39. This is an update on a research paper published in 2010 by Bradshaw, Simon and Millard, Christopher and Walden, Ian, 'Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services' Queen Mary School of Law Legal Studies Research Paper No. 63/2010. Available at SSRN: http://ssrn.com/abstract=1662374 or http://dx.doi.org/10.2139/ssrn.1662374 .This research forms part of the QMUL Cloud Legal Project http://cloudlegalproject.org, Centre for Commercial Law Studies, Queen Mary University of London.

[28] Bradshaw S, Millard C and Walden I in 'Standard Contracts for Cloud Services' in Millard (ed.), Cloud Computing Law (2013, OUP Oxford), 39.

[29] Reed, Chris et al., "*Report of survey of cloud contract terms*", Cloud Accountability Project D: D-4.2, Gleeson et al. (eds.), 2015.

	Term	What it means in a cloud contract
1	Applicable law	Clause setting out the relevant law for interpreting the terms in the contract
2	Jurisdiction	Clause setting out the court where any disputes over the contract will be held
3	Arbitration	Clause providing that disputes will be resolved by arbitration rather than litigation.
4	Acceptable Use	Clause or policy defining what the provider considers as acceptable use of the cloud service.
5	Variation of contract terms	Clause permitting variation of contract terms by the service provider.
6	Data integrity	Clause putting the responsibility for ensuring the confidentiality and integrity of personal data onto the customer and not the cloud provider.
7	Data preservation	Clause defining the obligations on the service provider to retain or to delete customer's data after the relationship with the cloud provider ends.
8	Data disclosure	Clause setting out the circumstances in which providers will, or may, disclose customer information to Law Enforcement Agencies (LEAs) and courts.
9	Data location/transfer	Clause setting out where customer data is stored (for example, location of data centre) and how it will be transferred (encrypted or not).
10	Monitoring by provider	Clause describing if and how the cloud service provider will monitor the customer's use of the cloud service.
11	IP Rights over service or content	Clause asserting IP rights over content and data uploaded to the cloud by customers.
12	Proprietary rights and duties	Clause asserting ownership of data stored in or processed via the cloud provider services.
13	Warranty	The warranty or guarantee given by the service provider to the customer for the performance of the service.

14	Direct liability	Clause concerning liability by the cloud service provider for losses to the customer relating to the loss or compromise of data hosted on the cloud service.
15	Indirect liability	Clauses concerning liability for indirect, consequential, or economic losses arising from a breach by the cloud provider.
16	Limit of liability	Clause limiting the extent of any damages or compensation that the provider may be liable for breach.
17	Indemnification	Clause that indemnify the provider against any claim against the provider arising from the customer's use of the service.
18	Service availability	Clause that specify a service performance target by the cloud service providers.
19	Service credits	Clause that give compensation to customers for failing to deliver the service to set levels by service credits, allowing the customer a rebate against future billing.
20	Terms of payment clause	Whether the contract has a periodic payment clause or not.

Table 1: Terms

3.2 Analysis of 20 typical contract terms

For the purpose of explaining how the analysis is conducted and how the rest of this section will be presented, we analyse each of these contract terms separately in four steps. First, we explain the purpose of the contract term in a typical cloud contract. We try to explain it in terms of the rights and obligations it gives a user of COAT. Second, we give an anonymous example of a typical term from a cloud contract from 2015.[30] We do not name the source contract because the focus is on the contract term, rather than any particular cloud providers' terms. Third, we give a view on the contract term from the perspective of accountability. Fourth, we suggest a best practice or a better alternative from an accountability point of view.
1. Applicable law

Explanation

The majority of cloud contracts include a term that provides that the contract is governed by the law of a specific jurisdiction. This is often, but not always, the law of where the provider has its principal place

[30] We choose what is a typical or representative example of each contract term from the range of cloud contracts surveyed as part of the Deliverable on Standard Contracts and SLAs.

of business. For example, out of the 31 terms of service analysed in 2010 and 2013, just over half of the providers specified the law of a particular US state.[31] The 30 terms of service surveyed in 2015 repeated this trend: most of the US cloud providers surveyed gave the governing law as being the law of a US state.

Example of an Applicable Law clause

Below is an example of a typical applicable law clause from a 2015 standard cloud contract:

This Agreement will be governed solely by the laws of the State of [US State], without reference to any principle of conflicts of law that would apply the laws of another jurisdiction to the parties' rights or duties.

Analysis from the point of view of accountability

The applicable law is important from an accountability point of view because it concerns how the customer can resolve a legal dispute with the cloud service provider. If the choice of law is not in the customer's usual place of residence or business address, this has a negative impact on how the customer understands or interprets their legal obligations. This is particularly the case where the choice of law specifies another legal system and language. This clause is highly relevant to how easy or difficult it is to bring a legal claim against the cloud service provider. Overall, the choice of law clause can contribute considerably to a feeling that there is less accountability, because there is less remediability where the choice of law is not in the customer's place of residence or business.

2. Jurisdiction

Explanation

The choice of forum or courts for settling disputes between the provider and customer is very similar to that of choice of law. The 2010, 2013 and the 2015 surveys[32] all indicate that providers specify a jurisdiction compatible with the specified legal system. In many cases, where the law of a particular US state is given as applicable law, the provider will include a term stating that claims against it must be brought in the courts of a particular city in that state.

Example of jurisdiction clause

This Agreement will be governed by and construed under the laws of the State of California, without giving effect to such state's conflict of laws principles. Any legal action or proceeding related to this Agreement shall be instituted in a state or federal court in Santa Clara County, California.

Or

The Agreement is governed by the laws of England and Wales and is subject to the exclusive jurisdiction of the Courts of England and Wales

Analysis from the point of view of accountability
Jurisdiction for a dispute is relevant to accountability since it relates to remediability and how difficult or easy it makes it for the customer to bring a legal dispute against the cloud service providers. The location of the court is a key factor in how a customer is able to get a remedy in any dispute with the cloud service provider. Since most cloud service providers have jurisdiction clauses based on where the cloud service provider has its place of business, this means that many customers are required by contract to bring disputes in courts outside of their jurisdiction. This is a significant barrier to accountability. Going to court in another jurisdiction creates an obstacle to bringing a dispute to court because it increases the cost of litigation for the customer. The customer has to incur travel expenses to appear in court and

[31] See Bradshaw, Millard and Walden, at 46, with a table setting out the breakdown of choice of law per jurisdiction for 2010 and 2013.

[32] For the 2010 and 2013 see Bradshaw, Millard and Walden, at 46, with a table setting out the breakdown of choice of law per jurisdiction for 2010 and 2013 and 47-48 describing how jurisdiction is generally compatible with choice of law. These findings were mirrored in the 2015 survey, D4.2 Deliverable (30 June 2015), at 18-19.

has to instruct foreign counsel to represent it in court. It may have to pay translation costs for any court proceedings or to produce evidence for the foreign court. Consumers may be protected by consumer protection legislation so that they can bring disputes to their local court. However, the business customer is not protected by such legislation and it is unlikely that any average business customer will undertake the risk and expense of foreign litigation. Therefore, the fact that the majority of jurisdiction clauses follow the applicable law clause, means that nearly half of all providers specify the law of a US state, irrespective of where their customers are located.

3. Arbitration

Explanation

Arbitration clauses are common in commercial contracts as an alternative to bringing disputes to court. Some cloud computing standard contracts give the option of commercial arbitration as an alternative to litigation and some, although a minority, require disputes between cloud service providers and customers to go to commercial arbitration rather than to court. The survey in 2015 indicates that over a quarter of cloud service provider included some type of clauses seeking to impose arbitration to resolve disputes.[33] Most of the arbitration clauses make reference to a forum for arbitration or recognized rules of arbitration, usually the American Arbitration Association rules.[34]

Example of arbitration clause

Any controversy or claim arising out of or relating to the Terms shall be settled by binding arbitration in accordance with the commercial arbitration rules of the American Arbitration Association. Any such controversy or claim shall be arbitrated on an individual basis, and shall not be consolidated in any arbitration with any claim or controversy of any other party. The decision of the arbitrator shall be final and unappealable. The arbitration shall be conducted in California and judgment on the arbitration award may be entered into any court having jurisdiction thereof.

Analysis from the point of view of accountability

Arbitration is relevant to accountability since it relates to the attribute of remediability. Arbitration is an alternative method of dispute resolution so it impacts on the way in which a customer can seek a remedy against its cloud provider. Consumer protection legislation in the UK means that any clause that forces consumer customers to go to arbitration is potentially unenforceable. Business customers, however, are not protected by consumer legislation and so would not have this defence against a compulsory arbitration clause.

Arbitration may suit a business customer better than having to file in a foreign court, since arbitration procedures are often more flexible than court hearings and allow the parties to have hearings by video conference, to agree on choice of language and to set dates for hearings in a flexible manner. Nevertheless, it is relevant to accountability because any customer should have the choice of arbitration. Arbitration that is imposed on the customer means that it has no choice of where to bring a dispute. In addition, the big disadvantage of arbitration is that there is no appeal procedure.

4. Acceptable use clauses

Explanation

Acceptable use clauses set out rules about how customers may use a service. They are sometimes set out in a separate document from the terms of service, called an Acceptable Use Policy (AUP),which contains a detailed list of prohibited behaviour by customers. Although the acceptable use clause or AUP appears to vary significantly in length and detail between different cloud service providers, they

[33] Consistent with the surveys in 2010 and 2013, Millard (ed.), 48-49.

[34] Only one did not use the US rules, New Zealand provider Mega used the New Zealand Arbitration association rules.

tend to prohibit the following range of activities: spam, fraud, gambling, hacking, hosting content that is obscene, defamatory or illegal or discriminatory.[35]

Example of clause

You agree to be solely responsible for the contents of your transmissions through the Services. You agree not to use the Services for illegal purposes or for the transmission of material that is unlawful, defamatory, harassing, libellous, invasive of another's privacy, abusive, threatening, harmful, vulgar, pornographic, obscene, or is otherwise objectionable, offends religious sentiments, promotes racism, contains viruses, or that which infringes or may infringe intellectual property or other rights of another. You agree not to use the Services for the transmission of "junk mail", "spam", "chain letters", “phishing” or unsolicited mass distribution of email. We reserve the right to terminate your access to the Services if there are reasonable grounds to believe that you have used the Services for any illegal or unauthorized activity.

Analysis from the point of view of accountability

The inclusion of an acceptable use clause by the cloud service provider is often an attempt to protect itself from liability arising from the illegal behaviour of their customers. From an accountability point of view, the explicit exclusion of certain illegal activities is probably of no importance to the majority of customers who want to use the cloud service for legitimate reasons. Where there is ambiguity about certain behaviour, explicitly excluding it or giving examples may help a customer understand what is meant by an exclusion.

5. Variation of contract terms

Explanation

Nearly all cloud providers surveyed in 2015 have a term allowing their terms of service to be varied. The majority provide that they may amend their terms of service by posting an updated version on their website and that continued use of the service by the customer was considered as their consent or acceptance of the new terms. Some providers stated that they would email customers about any material contract changes, but that continued use of the service constituted consent to the contract changes.

Example of clause

[Cloud Service Provider] reserves the right to modify these Terms at any time, and each such modification will be effective upon posting on the Site. All material modifications will apply prospectively only. Your continued use of any Products following any such modification constitutes your agreement to be bound by the modified Terms. To stay informed of any changes, please review the most current version of these Terms posted on the Site. If you do not agree to be bound by these Terms, you must stop using the Products immediately.

Analysis from the point of view of accountability

The accountability attribute is transparency since the contract changes need to be transparent for the customer to understand what has changed in its contract. This practice of sending posting a unilateral notice of changes to the cloud customer, by posting of contract changes on a website, is not accountable behaviour by cloud service providers. Nevertheless, prolonged contract negotiation following each contract revision with each customer is not feasible or even acceptable for the majority of cloud customers. Customers could be overwhelmed if they were asked specifically about each single amendment of contract and the majority of customers could be entirely indifferent to minor contract changes. However, placing the onus on the customer to check the website for potential contract changes

[35] Bradshaw et al, 48, note that the differences between acceptable use clauses and cloud service providers are about the level of detail in describing these activities, rather than the activities prohibited. Most clauses prohibit exactly the same range of behaviour.

is not appropriate and does not demonstrate accountability. Therefore, a balance needs to be struck between giving information to customers in an accountable way about contract changes and having a proportional response by cloud service providers.

6. Data integrity

Explanation

A data integrity clause in cloud contracts is generally written like a disclaimer so that the cloud provider is not responsible for data integrity and confidentiality. The majority of providers surveyed in 2015 included terms that the customer was responsible for preserving the confidentiality and integrity of the customer's data. Although some providers made reference to their 'best efforts' to preserve data integrity, they still made it the responsibility of the customer. Clauses in contracts surveyed in 2013 contained similar exclusions.

Example of clause

[Cloud Service Provider] agrees to maintain reasonable and appropriate measures related to physical security to protect Customer Content. Other than responsibility for physical security, Customer shall be solely responsible for data maintenance, integrity, retention, security, and backup of the Customer Content. You are responsible for the confidentiality of your account information and for all activities that occur under your account. You are solely responsible for all content within your account.

Analysis from the point of view of accountability

The data integrity clause is relevant to accountability since it relates to responsibility for processing data, potential sensitive personal data. The cloud service provider as a processor, and potentially as a data controller, has a regulatory responsibility that it cannot just exclude by a contractual clause. Although the cloud provider cannot be responsible for actions by the customer that lead to loss of data integrity and confidentiality, it also plays a role and the customer is not solely responsible for this.

7. Data retention and deletion

Explanation

These clauses govern what will happen to customer's data after the relationship with the cloud provider comes to an end. There are two issues: first, data portability, whether the customer can access data and use it elsewhere once the contract with the cloud service provider has ended; second, data preservation or deletion, whether the cloud provider undertakes to delete customer data after the end of the contract. As regards the issue of data portability, this is important for customers who want to transfer or recover their data in a managed manner. The surveys of cloud contracts found that providers dealt with the issue of how to deal with customer information following the end of the relationship between them and the customer, in the following three ways:[36]

- Providers retain customer data for a set period after the end of the contract, often 30 days.
- Providers delete customer data immediately at the end of the customer relationship.
- Providers state that there are under no obligation to preserve data after the end of the contract, but do not say that they will delete it or they state that a grace period before deletion may apply at their discretion.

Example of clause

Upon request by you made within 30 days after the effective date of termination or expiration of this Agreement, We will make the Your Data available to You for export or download as provided in the

[36] Bradshaw, Millard and Walden, 53, describes the results of the 2010 and 2013 surveys as regards data retention clauses by cloud service providers. The results of these surveys are reflected in the results of the 2015 survey conducted as part of the A4Cloud project.

Documentation. After that 30-day period, We will have no obligation to maintain or provide Your Data, and will thereafter delete or destroy all copies of Your Data in Our systems or otherwise in Our possession or control as provided in the Documentation, unless legally prohibited.

Analysis from the point of view of accountability

Reversibility/portability: guarantee the easy reversibility or portability of the data in a structured and widely used format, at the customer's request and at any time.[37]Many customers require limited and reasonable retention period for the data with regard to the purposes for which the data have been collected; just so that they can transition data between their cloud service and other service providers. Alternatively, depending on the data that they are storing, it may be sufficient that the provider deletes it on termination of their contract particularly if their contract is not a long-term contract. Even after deletion, data may still be read by certain software (for example used in computer forensics). If a customer has personal sensitive data, they may want to have greater certainty that the data is deleted permanently by having it overwritten. What most customers need is reversibility/portability: guarantee the easy reversibility or portability of the data in a structured and widely used format, at the customer's request and at any time.[38] In addition, they need a grace period before their data is deleted after the contract ends. This means transparently stating how long the data will be preserved; and being responsive to the customers need to port or to ensure deletion of certain data.

8. Data disclosure to Law Enforcement Agencies (LEAs)

Explanation

Some clauses cover the circumstances in which providers will, or may, disclose customer information including customer data stored on the provider’s cloud to law enforcement authorities. All providers surveyed say that they will disclose this data in response to a valid court order.[39] In respect of disclosing information in other circumstances, there is a spectrum of responses from providers concerning disclosure. Some cloud service providers adopt the strategy that they will disclose data to Law Enforcement Agencies (LEAs) if it exposes them to legal liability or if it is in order to protection the interests of a third party. Recent requests for information by US law enforcement agencies for information hosted in the EU have caused legal controversy and this point is being tested in the US courts.[40]

Example of clause

Disclosure to Law Enforcement
The Terms of Service specifically prohibits the use of our service for illegal activities. Therefore, Subscriber agrees that [Cloud Service Provider] may disclose any and all subscriber information including assigned IP numbers, account history, account use, etc. to any court who sends us a valid Court Order, without further consent or notification to the Subscriber.

Analysis from the point of view of accountability

[37]CNIL, ‘’*Recommendations for companies planning to use Cloud computing services*’’, available at http://www.cnil.fr/fileadmin/documents/en/Recommendations_for_companies_planning_to_use_Cloud_computing_services.pdf”

[38]Ibid

[39] For contracts surveyed in 2013 provide that they will disclose such data in response to a valid court order. Bradshaw, Millard, Walden, 54. Similarly in all contracts surveyed in 2015 show a similar result.

[40] Microsoft’s has entered into a legal battle against a US government request for access to emails from a Microsoft customer that are currently sitting on a server in Dublin, Ireland, as part of a narcotics investigation. In 2014, a US court ruled that Microsoft should hand the data over. Microsoft declined to comply, voluntarily entering into contempt. Several other technology companies have joined in the case on Microsoft’s behalf see http://www.theguardian.com/technology/2014/dec/15/microsoft-email-warrant-lawsuithttp://www.theguardian.com/technology/2014/dec/15/microsoft-email-warrant-lawsuit

Disclosure for law enforcement in circumstances where there is a valid court order is can be reasonable[41]. Disclosure to LEAs in other circumstances, particularly where the cloud provider has a lot of discretion about disclosure, pose more problems from the point of view of accountability. Where the cloud provider reserves the right to disclose to LEAs at its discretion or where it judges that there is a risk to itself of legal liability or to third parties, this means that the customer is not sure when and in what exact circumstances its information will be disclosed to LEAs, and also whether it will be informed of any such disclosure.

9. Data location and transfer

Explanation

One of the major legal concerns for cloud customer is where its data may be stored or processed since cloud provider can potentially transfer data anywhere globally to be stored or processed in global data centres. The legal position in the EU is that the EU data protection regime prohibits transfer of personal data out of Europe where there are inadequate protection for personal data.[42] However, most cloud providers surveyed do not state explicitly in their terms of service where they will store data. This is sometimes part of the sign up process: where users may be able to chose a region where their data is stored. Some providers indicate compliance with the US Safe Harbor obligations.[43]

The other concern for customer is whether it their data is protected in transit. Transfer of customer data between the customer and the cloud provider is usually over the Internet. Some providers' terms of service highlight that this is insecure if transferred unencrypted. Most providers, however, do not mention this issue at all in the contract.

Example of clause

Content Stored in the United States: The Services are available worldwide and currently hosted in the United States through our sub-processor XXX Inc. and other service providers. XXX Inc. is, and will remain, a certified member of the EU and Swiss Safe Harbor Frameworks, operated by the U.S. Department of Commerce and enforced by the Federal Trade Commission ("Safe Harbor"), and as such adheres to the EU and Swiss Safe Harbor Principles with respect to the transfer, processing and security of any personal data transferred from the European Economic Area or Switzerland. By submitting any personal information to us or our designees pursuant to these Terms or in connection with the use of the Services you consent to the collection, processing, transmission and disclosure of such information and related data by XXX within its group of companies and authorised service providers pursuant to these Terms both within the European Economic Area and outside (including the USA) in order for XXX to perform its obligations. XXX reserves the right to store and process information outside of the European Economic Area and United States, and will use commercially reasonable efforts to provide you with at least 30 days' notice of any such changes in the storage locations. Where you do not consent to such processing, you may terminate your Contract with us with immediate effect on written notice to us.

Analysis from the point of view of accountability

This is a key issue for cloud customers. Customers require transparency about where their data will be stored or transferred, particularly if they have regulatory obligations themselves about the data they are storing in the cloud (for example, it is their customers' or employees' personal information). Asking cloud customers to choose where they wish their data to be stored enhances accountability in the cloud, in the sense that it links to one of the earlier accountability attributes identified by the project, transparency.

[41] Note that the issue of access to the cloud by law enforcement agencies is highly complex, especially, in cases of LEAs wishing to access CSPs located in EU processing personal data of European citizens. Given, though, that law enforcement does not fall under the project's scope, this issue will not be discussed further in this deliverable.

[42] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31 (DPD)

[43] For example, one provider surveyed, Akamai provides on its website 'Privacy and Other Policies' includes a safe harbor agreement policy and is available at http://www.akamai.com/html/policies/index.html

Many service providers chose to avoid it, possibly for fear of incurring liability where they switch data from one service centre to another without verifying for each customer that they have consented to have their data hosted in the particular jurisdiction where the data centre is located.

10. Monitoring by provider

Explanation

Providers sometimes monitor the use of the cloud service by their customers, in particular to see whether they are complying with acceptable use policies. Providers are also often concerned about hosting illegal or otherwise inappropriate content and may monitor for this reason. Other providers may monitor customer use to assess the frequency and volume of data movement – traffic data and bandwidth consumption – just to ensure a good quality of service. Some provider cloud contracts, but not all, contain a clause where the provider acknowledges that it will monitor customer data and states the purpose of such monitoring.

Example of clause

Although [Cloud Service Provider] does not regularly monitor the use of its services by any particular user, it reserves the right to do so if [Cloud Service Provider], in its sole discretion, determines there may be misuse as defined by the terms of this Agreement. [Cloud Service Provider] may monitor Your access, use, files and/or Storage Data to detect signs of misuse.

Analysis from the point of view of accountability

Accountability depends on transparency and therefore a clause in the contract acknowledging that the cloud provider is monitoring customer data is positive. In addition, it is also transparent if the purposes of the monitoring are acknowledged: enforcement of the acceptable use policy; technical and quality measuring; or some other reason. If for whatever reason, the customer is concerned about monitoring of its data, it should be given options about this practice as, for instance, that only the metadata of the entrusted information to the cloud service provider is monitored, but not the actual content.

11. IP Rights over service and content

Explanation

This clause appears in contracts concerning intellectual property (IP) rights over content and data uploaded to the cloud by customers. Most cloud contracts that deal with this issue contain a clause that is reciprocal: it provides that the cloud provider retains IP in the service and that third-party content on the service remains the property of the content owner. This means that IP in customer data remains with the customer.

Example of clause

This Agreement does not grant Customer any intellectual property rights or licenses, including without limitation licenses to software incorporated into or accessed through the Services, to logos or trademarks associated with the Services, or to other written or graphical content provided by or through the Services.

Analysis from the point of view of accountability

No particular impact from accountability.

12. Proprietary rights and duties

Explanation

This is a catch-all category for clauses concerning proprietary rights and duties other than IP rights over customer content and service. This issue is not dealt with by the majority of cloud providers and so is not a feature of standard cloud contracts surveyed in 2015.

Analysis from the point of view of accountability

In general, clauses covering proprietary rights and duties feature in a very limited number of standardized cloud contracts and, therefore, it is being argued that they do not have an impact on accountability within a cloud environment.

13. Warranty[44]

Explanation

A warranty can have various meanings in contract law but it generally means a guarantee or promise by one party to the other party that specific facts or conditions are true or will happen. For example, a warranty given by a cloud computing provider to a customer regarding fitness of purpose or reliability of the cloud service. All cloud providers surveyed in 2015 that referred to warranty gave wide disclaimers often claiming that there was no warranty. There was a difference between contracts based on US law, where the disclaimer against the warranty was far more sweeping and comprehensive, and those where providers that claimed European jurisdiction referred sometimes to the fact that the disclaimers did not affect the customer's statutory rights or that they did not affect applicable legislation.

Example of clause

You expressly understand and agree that the use of the services is at your sole risk. The services are provided on an as-is-and-as-available basis. XXX expressly disclaims all warranties of any kind, whether express or implied, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. XXX makes no warranty that the services will be uninterrupted, timely, secure, or virus free. Use of any material downloaded or obtained through the use of the services shall be at your own discretion and risk and you will be solely responsible for any damage to your computer system, mobile telephone, wireless device or data that results from the use of the services or the download of any such material. No advice or information, whether written or oral, obtained by you from XXX, its employees or representatives shall create any warranty not expressly stated in the terms.

Analysis from the point of view of accountability

The clause limiting liability relates to accountability in respect of the attribute of remediability. This clause explicitly limits the scope of any remedy available to a cloud customer.

14. Direct liability

Explanation

A clause dealing with direct liability provides that the party in breach is liable for any loss or damages that a reasonable, ordinary, and prudent person would expect the non‑breaching party to suffer from a breach, where the reasonable, ordinary, and prudent person, though comparable to the breaching party, is a stranger to this particular contract. All cloud providers surveyed in 2015 exclude liability, although those in the US are more overt than in Europe. Several providers specify exactly what is included in direct breach for the avoidance of doubt. In most cases, particularly in contracts with US providers, these

[44] Note that the clauses regarding warranties, direct and indirect liability, liability cap and indemnification vary significantly in Civil law countries, such as Netherlands. Those issues will be discussed further under '*'D-4.4 Remediation guidelines and tools*'', A4Cloud project deliverable, forthcoming.

clauses are in capital letters so that the disclaimers on liability are conspicuous and not hidden in the contract.[45]

Example of clause

To the maximum extent permissible under applicable law, regardless of the legal theory under which liability is asserted and regardless of whether XXX has been advised of the possibility of liability, loss or damage, XXX, its licensors, affiliates, agents, and contractors will not be liable to you for any incidental, indirect, special, reliance, punitive or consequential damages of any kind (including, without limitation, any loss of use, loss of business, lost or imputed profits or revenues, loss or destruction of content, information or data, costs of cover, interrupted service, or reliance upon the software and/or associated documentation) arising out of or related to this agreement, service or software.

Analysis from the point of view of accountability

The clause limiting liability relates to accountability in respect of the attribute of remediability. This clause explicitly limits the scope of any remedy available to a cloud customer. The problem is that when this clause is very extensive it prevents the customer claims a remedy for injury or damage that is directly related to the contract breach. This is potentially unfair, and because of the imbalance in bargaining power, it is difficult for small business or consumers to argue against a widely drafted clause limiting liability. In the case of consumers, they may be protected under consumer protection legislation and may consequently be able to argue that the clause is unenforceable. Small or medium sized businesses are less protected.

15. Indirect liability

Explanation

Direct losses or injuries that are foreseeable consequences of the breach of contract fall within direct liability. Direct damages or losses can be reasonably anticipated as a consequence of the breach. In contrast, in English law, indirect losses concern losses that are more remotely connected with the breach of contract. These losses may result from knock-on effects of the breach of contract and, generally, it is not justifiable to make defendants pay for these losses because they are too remote, i.e. there was nothing to alert them that these losses would arise from the breach. The defendant will only be liable if there are special circumstances known to them at the time of the contract such that a breach would be liable to cause more loss. For example, if the cloud provider knows that a data or security breach will meant that the customer will automatically lose a lucrative government contract; or that a service failure means it incurs penalties for late delivery to its customers. In these circumstances, the defendant knows that these losses will occur if the contract is breached. Such losses (loss of a lucrative contract; payment of penalties for late delivery under contract) are indirect since they are not directly foreseeable consequences of the cloud security breach or system failure.

Indirect losses may cover a wide category of loss or damage and can include physical damage, loss of profits, economic losses and damage to goodwill and reputation. Most cloud contracts try to exclude indirect losses because they are unpredictable. They represent un-quantified and unidentified areas of risk for anyone entering into a contract. All cloud contract surveyed in 2015 excluded liability for indirect losses, often in very wide terms and in capital letters (all caps).

Example of clause

You expressly understand and agree that the Company shall not be liable for any direct, indirect, incidental, special, consequential or exemplary damages, including but not limited to, damages for loss of profits, goodwill, use, data or other intangible losses (even if the Company has been advised of the possibility of such damages), resulting from: (i) the use or the inability to use the service; (ii) the cost of procurement of substitute goods and services resulting from any goods, data, information or services purchased or obtained or messages received or transactions entered into through or from the service;

[45] This reflects the Uniform Commercial Code in the US. As a result, many warranties and disclaimers are in capital letters in contracts.

(iii) unauthorized access to or alteration of your transmissions or data; (iv) statements or conduct of any third party on the service; (v) or any other matter relating to the service.

Analysis from the point of view of accountability

The clause limiting indirect liability relates to accountability in respect of the attribute of remediability. This clause explicitly limits the scope of any remedy available to a cloud customer in respect of remote consequences of contract breach. Nevertheless, it is difficult to find fault in this practice, particularly in respect of contracts with business customers. It is entirely normal practice for any party entering into a contract to try to limit remote consequences of contract breach and cloud service providers are no different from other contractors. The only potential negative effect of such clauses is that they may too widely drafted, in particular, as regards contracts with consumers. The consequence of this however is likely to be negative for the cloud service provider, because the clause if too widely drafted may be held to be unenforceable by a court or in breach with consumer protection legislation. Therefore, there are no particular recommendations on best practice as regards clauses limiting indirect liability.

16. Limit of liability (liability cap)

Explanation

Clauses imposing a limit or cap on the amount that should be paid in the event that the person is liable for damages or loss. Over two-thirds of the cloud provider contracts surveyed in 2015 included a clause with a liability limit or liability cap, usually a multiple of what the customer paid in service fees over the previous 12 months with an upper limit. Those that did not mention a liability cap or limit usually had an absolute denial of liability and so did not need to set an upper limit. This type of liability cap is, however, unlikely to be enforceable in English or Irish law, particularly against a consumer.

Example of clause

To the maximum extent permitted by applicable law, [Cloud Service Provider]'s total liability and that of it its affiliates, officers, employees, agents, suppliers or licensors, arising under or in connection with the Contract: (a) for any Services for which no payment is due shall be limited to one hundred and eighty pounds (£180.00); and (b) in all other cases, be limited to the total fees paid by you to [Cloud Service Provider] for the specific use of the Services giving rise to the claim in the twelve (12) months preceding the event first giving rise to the claim under the Contract. For the avoidance of doubt, this liability cap shall not apply to any customers who are consumers.

Analysis from the point of view of accountability

The relevance of this clause to accountability is that it relates to the attribute of remediability because it restricts the remedy available to the customer in the case of loss or damage caused by the cloud provider. In addition, customer that are consumers and that often use free services means that this clause amounts to a denial of liability. Therefore, a liability cap is unlikely to be enforceable in English law against a consumer.

17. Indemnification

Explanation

An indemnity clause means that someone gives an obligation to provide compensation for future loss or damage. Consistent with previous surveys, a notable number of cloud providers surveyed in 2015 (over three quarters) asked their customers to indemnify the providers against any claims arising from the customer’s use of the service. Such an indemnity clause means that the customer is under an obligation to provide compensation for future damage, loss or injury suffered by the cloud service provider. Some cloud service providers also offered to indemnify the customer, for example, against claims for IP infringement arising from use of the cloud provider’s service.

Example of clause

[Cloud Service Provider] wishes to emphasize that in agreeing to the [CSP's] Terms of Service, customer indemnifies CSP for any violation of the Terms of Service that results in loss to CSP or the bringing of any claim against CSP by any third-party. This means that if CSP is sued because of a customer's or a customer of a customer's activity, the customer will pay any damages awarded against CSO, plus all costs and reasonable attorney's fees.

Analysis from the point of view of accountability

This relevance of this clause from the point of view of accountability is that it is transparent regarding the customer's potential legal responsibilities. It is a reasonable clause for any cloud service provider to include in a contract and, consequently, we have no recommendations for any changes or best practice from the point of view of accountability.

18. Service availability

Explanation

Service availability generally involves promising or undertaking a service performance target. However, for the majority of cloud providers surveyed in 2015, they explicitly excluded any service availability or performance levels. Several stated that they provided the service "as is" without promising anything further regarding its quality performance or availability. The rare cases where there was a service availability undertaking were in a Service Level Agreements (SLAs) that offer service credits for failure to reach the specified service level target.

Example of clause

Other than as expressly set out in these terms or additional terms, neither [CSP] nor its suppliers or distributors makes any specific promises about the Services. For example, we do not make any commitments about the content within the Services, the specific functions of the Services or their reliability, availability or ability to meet your needs. We provide the Services "as is".

Analysis from the point of view of accountability

This is another example of excluding responsibility for the service. In that sense, the only advantage of having such clause is that it increases transparency of CPS and, therefore, strengthens accountability in the cloud. Moreover, from a business perspective, especially, bigger companies would have the possibility –on the basis of such clause- for arguing for arguing for greater service performance availability in the context of a service level agreement.

19. Service credits

Explanation

Service credits are a way of compensating customers for failure to deliver the service to set levels. This is normally a feature for commercial services that instead of monetary compensation a reduction in the next bill is offered. This is typically included in a service level agreement (SLA) specifying the performance level and agreeing service credits where the performance failure to meet the required levels[46].

Example of clause

[46] Note that in a Civil Law country such as Netherlands, this particular issue of service credits might be regulated differently than within a Common Law country like the UK. Dutch Civil Code, for instance, dictates that the provisioning of service credits deprive customers from their rights for remedies. In order for cloud customers to be entitled to service credits maintaining their right for remedies, cloud contracts should explicitly dictate so.

For each 30 continuous minute period of Qualifying Outage Minutes for a Service in a Measurement Period, [Cloud Service Provider] shall provide a SLA Credit of 5% of the fees for the relevant Service which was subject to the Loss of Service during the Measurement Period. Any period of Qualifying Outage Minutes for a Service which is less than 30 continuous minutes shall not be eligible for an award of SLA Credits.

Analysis from the point of view of accountability

This is a way of providing a remedy to customers for service failure and so is related to accountability through the attribute of remediability. In addition, it provides an easy way of giving the customer a remedy without obliging them to take court action or engage in litigation.

20. Terms of payment clause

Cloud contracts with customers fall into two general categories. Customers opt for either a paid for service with a periodic payment clause or a free service.[47] For paid services, the contract sets out the initial duration of the contract, its renewal period and payment structure. Despite the fact that for free services there is no periodic payment structure, these services are offered for free only for a limited amount of time

Analysis from the point of view of accountability

This is no particular significance from an accountability point of view concerning payment terms in themselves in cloud contracts. The hidden “costs” of the free services are of great importance, since individual end users are often requested in return to agree having their personal data processed for advertising purposes; this, however, is beyond the scope of this particular piece of analysis. Note that given that COAT compares cloud offered services, price will essentially be covered by the tool’s questionnaire.

3.3 Variations of clauses

The extent to which the earlier discussed clauses differentiate across the service delivery models (SaaS, PaaS, IaaS) varies. Certain clauses remain almost unaltered irrespective of the delivery model, while others may differentiate. Given that the earlier stated survey primarily concerned standard cloud contracts offering SaaS services, the remarks summarized below are mainly drawn from literature review.

Acceptable use of the service constitutes an example of contractual clause varying depending on the type of service. Although the forbidden behaviours remain the same, the level of detail varies depending on the type of service being offered. Nevertheless, the aims of these provisions and the emerging consequences in case of non-compliance remain the same.

Furthermore, the emphasis put on data portability by SaaS contracts compared to cloud contracts for other services is self-explanatory; maintenance of format and of other characteristics of data is particularly important in case users of cloud services wish to export their data at the end of the contractual relationship. Similarly, the existence of multiple parties in the CSP's supply chain – subcontracting (e.g. meta providers) appears particularly important when considering the SaaS environment, given that this type of service is most likely to run on other providers' infrastructures or platforms.

Furthermore, while the Terms and Conditions relating to the cloud service availability (i.e. what is generally contained in the SLA) do not seem to have such a strong connection with the service model, but rather appear to depend on other (more precise) factors – eminently on the qualification of the service as free or as available under a certain fee –, the ones relating to the service's integrity and

[47] Bradshaw, Millard and Walden (2013), at 45, note that there is an element of overlap between the paid and ‘free’ services. So-called free services may involve non-monetary costs on the customers: for example, requiring customers to consent to license terms that allow re-use of customer’s data for its own purposes.

confidentiality appear to vary according to the service delivered model addressed. Also, the level of control a user can exert over the data it deals with influences its responsibilities with respect to the integrity and confidentiality-related aspects of the contractual relationship, and is different according to the service model considered, meaning highest level of control in case of use of a IaaS service and lowest in case of a SaaS.

On the contrary, amongst the contractual provisions we examined, it seems that the service model bears no influence on the applicable law and on the jurisdiction, those attributes being related to other considerations, nor on the clauses relating to the dispute resolution mechanisms. The Terms and Conditions which regard the possibility for the provider to change the contract's terms and the notification do not seem to relate directly to the service model adopted by the CSP remaining unaltered irrespective of the service delivery model.

4 Comparison websites for cloud services: the legal framework

This section assesses the law applying to cloud comparison websites in the EU and, in particular, in the UK. It looks at the legal and regulatory framework that a comparison website provider would need to take into account in setting up a cloud comparison website. It provides an overview of the main legal requirements for comparison websites, including the best practice guidance issued by various consumer and regulatory authorities. It uses this analysis to set out the legal framework to address when developing a cloud contract comparison tool, the Cloud Offering Advisory Tool (COAT).

4.1 Defining online comparison tools

Customers have access to a vast quantity of product and pricing information online. This wealth of information sometimes threatens to overwhelm them and complicates decision-making. Online comparison tools provide a useful and quick way to help decision-making by comparing various offers and, in some cases, finding the most suitable deal for the individual customer. Consequently, price and product comparison websites have proliferated in recent years and are used by increasing numbers of consumers.[48]

Online comparison tools encompass a variety of different websites and tools.[49] Examples of common types of comparison tools include price comparison websites, whether for particular products or for a wide range of consumer goods. Comparison websites may also be defined as a vertical or product specific search engine as opposed to a general search engine. The results allow consumers to filter and compare products or services based on price or other features and criteria. Some comparison websites are purely search tools, for example mere hyperlink providers, aggregating information from many different retailers. Others are like e-commerce platforms and act as a shopping gateway with a direct link to the sellers. Some offer automated online 'brokering services' that try to match the best offer to each user based on the user filling out details of their individual products or preferences. For the purposes of this paper we will use the term 'comparison tools' to cover all types of price comparison website, from mere hyperlink providers to the more sophisticated online brokering services.

The most common features of comparison websites are that the Internet user is required to complete a questionnaire or select suggestions from a list of options in order to determine their demands or needs.[50]The comparison websites then provide information to the Internet user based on their answers to the questionnaire or their selected options, usually with details about the price and the main features of a number of products or services.[51]

4.2 Legal framework for comparison websites

The legal and regulatory framework potentially covering comparison tools is extensive. Horizontally applicable rules that could apply to online comparison tools include unfair commercial practices and consumer rights laws, misleading and comparative advertising law, data protection laws and competition law.[52]In addition, in regulated sectors such as energy, financial services and communications, some of the sector regulatory authorities have issued codes of conduct for comparison websites in their sector and have sought to regulate aspects of price comparison websites.[53]

Contract and consumer law and comparison websites

[48] "Consumer market study on the functioning of e-commerce" (2011) conducted on behalf of the European Commission, DG Health and Consumers, by Civic Consulting.

[49] 'Comparison Tools – Report from the Multi-Stakeholder Dialogue' Providing consumers with transparent and reliable information (Report presented at the European Consumer Summit 18-19 March 2013), at 7, available at http://ec.europa.eu/consumers/documents/consumer-summit-2013-msdet-report_en.pdf

[50] Report on Good Practices on Comparison Websites, EIOPA-CCPFI-13/100, 30 January 2014, at 9.

[51] Ibid.

[52] European Commission 'Comparison Tools – Report from the Multi-Stakeholder Dialogue. Providing consumers with transparent and reliable information' (Report presented at the European Consumer Summit 18-19 March 2013), at 9-14 in Chapter 2 Regulatory framework at EU level.

[53] Ibid, p14-18.

The EU legal framework does not address the issues of comparison tools separately; there is no specific legal instrument that addresses comparison websites. Instead, a wide variety of EU legislation, mainly aimed at protecting consumers, is relevant to the analysis of the legal issues that arise when creating a comparison website.[54]

General legal instruments likely to impact comparison websites

The following is a summary of the main legal instruments that may apply to comparison websites, particularly those aimed at consumers.[55] The application of any specific piece of legislation to a website would, nevertheless, also need to be based on the business model and specific facts of how the website operated. For example some of the Directives listed below require that a comparison website provider is a 'trader' or 'acting on behalf' of a trader before the legislation would apply.[56] Therefore the application of any specific piece of legislation would depend on the particular circumstances of the case and whether the comparison website provider could be deemed to be involved in the sale of any product or service or to be 'acting on behalf' of any supplier of products or services recommended in search results on its website.

Main examples of horizontal legislation that could apply to price comparison websites include:[57]

- *Unfair Commercial Practices Directive*[58] – prohibits traders making false or misleading statements about the price or availability of products.[59] It requires that a trader is transparent about the independence of this business or if it is operated or sponsored by another business.[60] If the site is a commercial site then the definition of a trader in the Directive would apply here.[61]

- *Consumer Rights Directive*[62] - this protects consumers buying online, and so would apply to comparison websites that sell services. It requires that detailed pre-contractual information be made available to the consumer about a range of matters that include price, payment, delivery, performance, contract duration, conditions for termination and right of withdraw from the contract. In most cases, the Consumer Rights Directive will not apply directly to the comparison website, since it is only acting to introduce customers to third party service sellers. However, the provisions of the Directive are still important because the comparison sites summarise terms and conditions and product features and misdescription could lead to liability for the service provider. In addition, in some cases, the comparison site may be acting as an agent for the service provider, and consequently may incur liability under the Directive.[63]

- *Misleading and Comparative Advertising Directive*[64] – This prevents advertising that is misleading and it sets out a list of conditions that comparative advertising should meet, for example, it should not discredit or denigrate the goods or services of competitors.[65] It prohibits discrediting competitors or taking advantage of their reputation in making comparisons.

[54] Ibid MSDCT report.
[55] ibid MSCCT report, 9.
[56] ibid MSCCT report, 9.
[57] Ibid MSDCT report 9-13
[58] Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market.
[59] Articles 6 and 7
[60] Ibid.
[61] Article 2(b).
[62] Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights
[63] Recital 16 of the Directive provides that national law applies on whether a person is considered an agent of a trader or not. Therefore, the application of the CRD varies depending on national law on agency and whether an entity can be considered an agent or not for a trader.
[64] Directive 2006/114/EC of the European Parliament and of the Council of 12 December 2006 concerning misleading and comparative advertising.
[65] Ibid, Article 4.

- *Data Protection Directive*[66]– This applies to personal data and protects how it is processed, gives rights to data subjects and imposes requirements on data controllers about how they process data. The comparison website will inevitably be a data controller within the meaning of the Directive and so will be subject to the requirements in the Directive to process personal data.

- *E-Commerce Directive*[67] – This applies to providers of 'information society services'[68] and most comparison website providers would fall within this category. It requires that such providers need to ensure that specified information is easily, directly and permanently accessible to recipients of the service they provide i.e. that they provide the name of the service provider, their contact details on their website, the details of their trade registration and VAT number.[69]

"Good practice" guidance for comparison websites

In general, consumer law enforcement agencies and consumer bodies view online comparison tools positively because these tools facilitate greater choice by consumers.[70] Prior to comparison websites, comparing suppliers meant that the customer had to submit information to each supplier to get a quote, particularly for service supply quotes that rely on the individual's personal data (for example, life insurance quotes).[71] In contrast, the online customer using a comparison website usually has to complete one questionnaire only and this is sufficient to receive quotes from various suppliers. Consequently, authorities are keen that consumers in particular continue to use price comparison websites.

The problem identified by various authorities is that some sites undermine customer confidence by lack of transparency, lack of clear information about the owner or operator of the site, and failure to implement a data protection policy or a complaints procedure.[72] These issues have led to customers being suspicious of the search results and less likely to trust comparison websites. For this reason, authorities have been keen to publish 'best practice' guidance for these websites as well as guidance for Internet customers using comparison websites.[73]

The issues identified in the UK Office of Fair Trading (OFT) report on Price Comparison Websites published in 2012 gives an analysis of cross-sectorial issues with comparison websites[74] and identifies the following legal issues: data protection and privacy, transparency of information, and exclusion of liability and complaints handling.[75] It has made recommendations to comparison websites based on each of the issues.

[66] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281, 23/11/1995, pp. 31 – 50.

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

[68] Article 1(2) of the Directive on electronic commerce defines information society services as any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services.

[69] Article 5 of Directive on electronic commerce.

[70] For example, the UK Competition and Markets Authority (which has replaced the UK Office of Fair Trading (OFT) since April 2014) finds that it is a 'key choice' tool in its paper 'Price comparison websites. Trust, choice and consumer empowerment in online markets' November 2012 (OFT 1467) and the Comparison Tools Report by the Multi-Stakeholder Dialogue group for European Commission DG for health and consumers; available at http://ec.europa.eu/consumers/documents/consumer-summit-2013-msdet-report_en.pdf

[71] European Insurance and Occupational Pensions authority (EIOPA) Report on Good Practices on Comparison Websites, EIOPA-CCPFI-13/100 30 January 2014

[72] OFT 1467, executive summary.

[73] Ibid OFT 1467 and MSDCT reports.

[74] This followed a web sweep by the OFT of 55 comparison websites designed to identify issues 'that could promote or undermine consumer trust' and a roundtable with regulatory and consumer bodies to discuss the results of the web-sweep. OFT 1467,11.

[75] OFT 1467, p 11.

Compliance with Data Protection Law

The OFT recommended that comparison website providers ensure that privacy policies are made clearer to users and that they implement the relevant Code of Practice published by the UK Data Protection Commissioner.[76] In particular, it advised that it should be clear to consumers that they could make an informed decision whether to opt out of data being shared with third parties or being used for marketing purposes.[77]

Transparency

The OFT found that comparison websites are not always transparent about how they arrive at certain search results, how these results are ranked and the effect of any commercial relationships on the ranking.[78] In addition, claims about the proportion of the market searched are often not clear nor appropriately qualified. In some cases, the comparison website does not explain the identity of the business operating the website. It concluded that omissions and misleading statements could breach both UK advertising codes and consumer contract laws.[79]

The OFT recommended that comparison website providers should take the following three actions to ensure transparency and compliance with the law:[80]

- *Clarity in presentation of search results* - The comparison website provider needs to be clear about the way search results are presented by explaining to consumers the basis of different search results. In particular, it needs to distinguish clearly comparisons based on objective criteria (for example, relevance or price) from promotions based on commercial relationships (for example, 'offer of the week'). Failure to disclose such commercial relationship where that information is material to a consumer's decision making may breach the law.[81]

- *Clarity about the nature of the search* - The comparison website providers need to explain market coverage since many statements overstate market coverage using "we've searched the market" when in fact there is only partial coverage.[82] In addition, the OFT recommends that the comparison website provider states how frequently it updates its information on prices and stock availability.[83]

- *Identification of the business operating the website* – Failure to identify the business operating the website is a breach of the Electronic Commerce Regulations 2002. Failure to disclose ownership links and commercial relationships with vendors of goods and services may also be in breach of the law. The OFT also found that over a quarter of consumers considered that comparison websites search results were based on who paid the website provider the most.[84]

1. Liability, complaints and redress

The OFT found that many websites include a general exclusion of liability in relation to search and comparison services which in many circumstances it found incompatible with the Unfair Terms in Consumer Contract Regulations 1999 (UTCCRs).[85] In addition, many comparison businesses gave no

[76] UK information Commissioners' Code of Practice for Personal Information Online http://ico.org.uk/for_organisations/data_protection/topic_guides/online/~/media/documents/library/Data_Protection
[77] OFT, 1467 at 19.
[78] OFT, 1467, 13.
[79]Committee of Advertising Practice's UK Code of Non-broadcast advertising, Sales Promotion and Direct Marketing (CAP Code) and the Consumer Protection from Unfair Trading Regulations 2008 (CPRs).
[80] OFT 1467, 21.
[81] The Code and the CPRs, OFT 1467, 15.
[82] OFT 1467, 15.
[83] Failure to do so is in breach of the CPRs, OFT 1467, 15.
[84] OFT 1467, 15, describing the results of the Advertising of Prices, December 2010, OFT 1291, annex Q, www.oft.gov.uk/OFTwork/markets-work/advertising-prices/#named4.
[85] OFT 1467, 17.

contacts details and had no complaints procedure so that it was virtually impossible for a consumer to contact some business to make complaints. It advised that failure
to provider material information in relation to complaints handling might breach the CPRs.

Competition law issues

Another area of law that has raised issues for online comparison websites is competition law. On the one hand, online comparison tools are potentially pro-competitive since they increase transparency for buyers.[86] On the other hand, sharing information on pricing has always been a sensitive subject in competition law. Competition law prohibits price-fixing agreements between market players or any behaviour that leads competitors to collude on price.[87] The relevant competition law in the EU is Article 101 of the EU Treaty[88] which prohibits agreements that restrict prevent or distort competition. Any agreement, including a contract between a comparison website provider and a supplier, could fall within this prohibition.

Competition law issues with comparison websites have arisen from the way in which the contract between suppliers and the online platform have led to restrictions on pricing through a ‘price relationship agreement’ or PRA in which the price terms are referenced to competitors. For example, if a seller gives a “price beat” guarantee to its customer, it agrees to beat any competitor’s price for the same or competing goods. The most well-known type of PRA is the ‘most favoured nation’ or MFN clause in which one party to a contract promises to give the other party at least as favourable contractual terms as it gives any other counterparty. For example, a seller may promise the customer not to sell to any other customer at a lower price.

Several competition authorities have opened a series of investigations concerning PRAs for online sales or concerning online platforms.[89] The UK OFT commissioned a report that identifies competition concerns that could arise from PRAs.[90] The controversy about MFN clauses has also led to an investigation of these clauses in contracts with providers of online comparison websites by the

[86] According to economic theory, social welfare is maximized in conditions of perfect competition. In the theoretical world of perfect competition, customers have access to information about all prices on the market and can freely access the product and price most appropriate for their needs. See Motta, Competition Policy: theory and Practice (Cambridge University Press, 2004); Bishop and Walker, *The Economics of EC Competition Law* (Sweet & Maxwell, 3rded, 2010); Carlton and Perloff, *Modern Industrial Organization* (Addison Wesley, 4thed, 2005).

[87] Whish and Bailey, *Competition Law* (Oxford, 7thed, 2011), Chapter 3.

[88] EU competition law applies to anti-competitive behaviour that affects a significant part of the EU. Most EU member states have also enacted national competition law laws (often based on the EU competition law prohibitions) that apply to anti-competitive behaviour that is limited to national or sub-national markets. For example, Chapter I of the Competition Act 1998 in the UK.

[89] The most widely publicised case on MFNs is the Apple e-books case where Apple and five publishers were investigated in the EU and US for using MFNs for sales of e-books. European Commission ‘Antitrust: Commission accepts legally binding commitments from Simon & Schuster, Harper Collins, Hachette, Holtzbrinck and Apple for sale of e-books’ European Commission MEMO/12/983, 13 December 2012. European Commission Press Release ‘Antitrust: Commission accepts legally binding commitments from Penguin in e-books market’ IP/13/746, 25 July 2013. For the US case see http://www.justice.gov/atr/cases/applebooks.html. In addition, online travel agents have faced several recent investigations by competition authorities in the UK and Germany concerning the use of MFN clauses by online search portals. In the UK, the UK accepted commitments from Expedia see OFT, ‘Hotel online booking: Decision to accept commitments to remove certain discounting restrictions for Online Travel Agents’ OFT 1514, 31 January 2014. The German Competition Authority (the Bundeskartellamt) has issued a ‘cease and desist’ order to online hotel portal operator HRS concerning the use of the MFN clauses see Press Release ‘Online hotel portal HRS's 'best price' clause violates competition law – Proceedings also initiated against other hotel portals’ dated 20 December 2013 and available at
http://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2013/20_12_2013HRS.html

[90] Lear, ‘Can “Fair” Prices Be Unfair?’ a report prepared for the OFT by Lear, September 2012, available at http://www.learlab.com/pdf/oft1438_1347291420.pdf . On the same subject, Lear has also published a Competition Note ‘Price relationship agreements: economic analysis for implications for competition’ November 2012 available at http://www.learlab.com/pdf/lcn_pra_final_textefigures_1354270080.pdf

Competition Commission in the UK. As part of a wider investigation into the motor insurance market,[91] it examined the use of MFNs in online comparison websites for private motor insurance.[92]

The Competition Commission considered the effect of the MFN clauses contained in the contracts between comparison websites and insurers. It categorized MFN clauses into two broad types: 'wide' and 'narrow'. 'Wide' MFNs are MFNs between price comparison websites and insurers which require parity (the same or a better price) with all competing price comparison website and the insurer's own direct channel (and in some cases in any sales channel at all).[93] Narrow MFN clauses specify that the insurer's own website will not offer policies at a lower premium than available on the price comparison website.[94]

The Commission found that price competition was weakened because of wide MFN clauses between price comparison websites and insurers. The usual strategy for a new entrant seeking to gain a foothold in the market is to offer a cheaper product, but this strategy is precluded by a wide MFN clause.[95] Consequently, the wide MFN clauses meant that there was less price competition and the result is that consumers pay higher motor insurance premiums.[96] The Commission did not however, rule out the use of MFN clauses. It recognised that narrow MFN clauses, but not wide ones, may be necessary for the survival of a price comparison website business model.[97] This is because a narrow MFN provides that lower prices cannot be found simply by going to the direct website of the insurer, and this lends credibility to the price comparison website and reassures consumers that the comparison website can be trusted.[98] Without a narrow MFN clause a retail consumer could bypass the comparison website and go directly to the insurer's website and so undermine the business model of the price comparison site.[99]

The Competition Commission's analysis of the potentially anti-competitive effects of MFN clauses used by comparison website providers is more widely applicable than the insurance market. In particular, the distinction between the wide and narrow MFN clauses in contracts between comparison website providers and sellers is highly pertinent to comparison website providers in any field, including cloud.

4.3 Cloud comparison tool for accountability

Several online comparison tools for cloud computing have been developed in recent years.[100] Some are simple price comparison calculators,[101] while others are more elaborate comparisons of different specific features of cloud, such as storage or hosting for example.[102] There are very few online comparison tools aimed at consumers or SMEs wanting to compare cloud service offerings on anything other than price. Unlike the COAT tool discussed later under Section 5, cloud comparison websites do not feature comparison based on how the CSP addresses data protection.

[91] On 28 September 2012, the Office of Fair Trading referred the motor insurance market and related goods and services in the UK to the Competition Commission for investigation and report under sections 131 and 133 of the Enterprise Act 2002. The Competition Commission is required to decide whether any feature of the market prevents, restricts or distorts competition and if there is an 'adverse effect on competition' in the market in accordance with Section 134 of the Enterprise Act.

[92]This investigation is part of a wider investigation by the Competition Commission in the UK into the private motor insurance market and related goods and services to decide whether any feature of that market there was an adverse effect on competition. See Competition Commission '*Private Motor Insurance Market Investigation*' Provisional findings report published on 17 December 2013.

[93] Ibid para 73.

[94] Ibid.

[95] Ibid para 77.

[96] Ibid, para 6.

[97] Ibid, para 80.

[98] Ibid, para 80.

[99] Ibid, para 81.

[100]Examples include Cloudorado, a cloud computing price comparison engine, available at http://www.cloudorado.com/

[101] For example, Cloud price calculator http://cloudpricecalculator.com/

[102] For example, PlanForCloud, a free online tool, tracks and calculates potential deployment costs with six different providers.

The A4 Cloud project has developed the COAT tool as an online comparison tool for cloud offerings aimed at consumers and at small and medium sized enterprises (SMEs).The purpose of the legal and regulatory analysis in this paper is to feed into the development of this tool.

The legal framework for the governance of comparison tools is equally applicable to cloud computing online comparison tools. The issues flagged by various regulators concerning best practice are equally relevant to cloud computing online comparison tools and COAT. These include:

- the requirement to have a ***complaints procedure and contact details*** easily accessed from the website of the comparison tool provider,
- the requirement to declare ***conflicts of interest*** clearly to the customer using the comparison tool on the website,
- the right to ***explain the rankings*** and the method for arriving at the rankings, and
- the requirement to have a ***data protection policy*** and make it available to all customers.

There are some issues in particular that may be useful to highlight for the COAT tool:

□ *Consumer vs. SME* - The COAT tool is designed for use by both consumers and businesses, albeit small and medium sized enterprises. A lot of the guidance on best practice for operating an online comparison website concerns consumers only, so some of the regulation would not be required by law in relation to SME customers using the COAT tool. The question is whether to differentiate in the standard of protection given to SME customers. It may be preferable to apply the standard of protection for consumers to all customers, irrespective of whether they are consumers or not, since this would provide uniformity and would protect all customers to the highest standard. Even if this imposed an additional burden that was not required by law, it would be consistent with the aim of the A4Cloud project by providing enhanced accountability to all customers, even when this is not required by law.

□ *Explaining cloud pricing* – Cloud is not a regulated market and so is not subject to sector-specific regulation. Nevertheless, one of the features of guidance by the sector regulators is that pricing and tariffing is explained by examples. For example, in assessing electricity prices, the energy regulators give an example of how these prices are calculated and what the different calculations mean. Each price comparison website is required to do similar, since consumers may not understand the terminology used by electricity suppliers on price comparison. Additional step-by-step guidance may be needed for customers to understand the choices they have when assessing cloud contracts. This may be particularly the case for SMEs who are buying various combined cloud offerings.

□ *Competition law and MFN clauses* - The contract between the comparison tool provider and the cloud providers that are suppliers to the comparison website needs to take into account the recent developments in competition law as regards price relationship agreements. Following the recent case law, the contract should avoid clauses that agree to restrict the price, especially if they are broad in scope, such as the wide MFN clauses. The anti-competitive impact of these clauses depends on the nature of the market so in the initial start-up phase of online cloud computing tools they may be innocuous. Nevertheless, since these clauses have been condemned in various cases, most recently in the UK, it may be advisable to err on the side of caution.

□ *Independent Audit* – This would make COAT itself accountable, and would set it up for accreditation if a national law or consumer enforcement body set up an accreditation scheme.

These steps could enhance the accountability of the COAT tool itself.

5 Cloud Offerings Advisory Tool (COAT)

The section below discusses COAT. It explains the selection process of attributes covered by the tool's questionnaire and discusses in detail the tool's architecture. Also, it presents briefly the feedback collected with respect to the tool in workshops organized by the project. Finally, it explores the way forward by explaining how COAT could benefit by the current development within the project of an Accountability Maturity Model.

5.1 Setting the scene for cloud brokers

The NIST cloud computing reference architecture describes the role of a cloud broker[103] as "an entity that manages the use, performance and delivery of cloud service and negotiates relationships between Cloud Providers and Cloud Consumers". The high level architecture of a corresponding cloud broker service in a federated cloud environment has already been analysed and developed (see for example[104] [105] [106] [107] [108]). Functionalities of a cloud broker typically include consolidated billing, seamless switching between providers, matching services with consumer requirements and monitoring. While the cloud broker definition is quite broad and still evolving, many companies (particularly those that were previously managed application service providers) are currently providing services that fulfil this role in the form of cloud (services) brokers: for example ComputeNext, Interworks, Nephos Technologies and TriCore Solutions[109]. In general, cloud brokers add value to one or more cloud services by means of one or more of the following[110]:

Aggregation: A cloud broker bundles many individual services and presents them as a unified service ensuring interoperability. For example, cloud brokers can offer a variety of security services from different vendors for a complete solution.

Integration: An enterprise will often rely on a cloud broker to integrate multiple services to achieve new features and functionality. A cloud broker can help move data into the cloud and integrate the customer's network with the provider's network as well as other partner networks.

Customization: A cloud broker often customizes cloud services for individual customers as well as customising the deployment of cloud-based applications.

The tool discussed in this deliverable is different from this, being an independent matchmaker service, connecting cloud users with suitable providers, and with no further follow-up. It does not connect to the cloud service on the client's behalf and manage the total packaged solution. Rather, it is more of a fully automated passive cloud broker functionality (in the sense that it brings out and matches what one side wants with what another side is offering) and moreover that provides privacy-centric guidance about the strengths and weaknesses of different cloud service provider (CSP) offerings as to which best meet an individual's expectations or a small organization's business requirements. Some similar systems are already being offered, although with greatly reduced functionality, notably CloudScreener.com[111], which provides ranked feedback about hosting a business application in the cloud, website hosting and data sharing and storage services, similarly based on selections that the customer makes via the website (without needing to establish a business relationship first).

5.2 Related Academic Work

There is a reasonably large, and growing, body of related academic work, the most relevant of which to the proposed system is the following:

[103] F. Liu et al, "*NIST cloud computing reference architecture*", NIST special publication, 500, p292, 2011.

[104] S.G. Grivas, T. U. Kumar & H. Wache, "*Cloud Broker: Bringing Intelligence into the Cloud: an Event-Based Approach*", Proc. CLOUD2010, IEEE, p. 544, July 2010.

[105] R. Buyya, R. Ranjan & R.N. Calbeiros, "*Intercloud: Utility-oriented federation of cloud computing environments for scaling of application services*", Algorithms and architectures for parallel processing, Springer Berlin Heideberg, pp. 13-31, 2010.

[106] "*CompatibleOne Open Source Cloud Broker Architecture Overview*", White Paper, Compatible One, Oct 2012.

[107] "*Integrating the Cloud: Bridges, Brokers and Gateways*", White Paper, f5 Networks Inc., 2012.

[108] N. Grozev & R. Buyya, "*Inter-Cloud architectures and application brokering: taxonomy and survey*", Softw. Pract. Exper. 2014, 44, pp. 369-390, 2014.

[109] Gartner, Cool Vendors in Cloud Services Brokerages, 2013.

[110] Gartner report, July 2009. http://www.gartner.com/it/page.jsp?id=1064712

[111] Cloud Screener: http://www.cloudscreener.com/en

1 Matching cloud user requirements to cloud services, e.g. via usage of an Service Level Agreement (SLA) template within a CFP[112], by matching to contract requirements and offerings specified in an XML schema extending WS-Agreement to security attributes [113] or by optimally mapping the requirements of users to published services [114] [115]. One approach is that of the EU FP7 Aniketos[116] project on secure and trustworthy composite services, including usage of algorithms to match certain security requirements (particularly confidentiality, integrity and trustworthiness) specified by service designers against service attributes specified in WS Security policies; however, this does not address the issue of how data are actually being used and protected within the solution provided. Another approach is being addressed in the EU FP7 SPECS project.

2 Autonomic acquisition of resources from providers on the basis of SLA evaluation rules, to help find the most suitable cloud provider that satisfies users' requirements, within the context of the EU FP7 MOSAIC project.[117][23] The Cloud Agency in the MOSAIC project is a broker that will assist applications in discovering cloud resource providers, negotiating SLAs with these providers and monitoring the SLA fulfilment, involving semantic and agent technologies.[118]

3 Cloud resource procurement taking into account dynamic pricing or risk/profit trade-offs.[119]

4 SLA@SOI[120] provides an open source based SLA management framework that can be used as a standardized basis for transparency and automation, although it is not a brokerage service.

5 EU FP7 OPTIMIS project: framework for brokerage based cloud services, including matching requirements of the cloud customer with offered cloud services, but also a number of other aspects including monitoring the performance with regard to the SLAs agreed. [121]

6 EU FP7 Contrail project[122]design and implementation of an open source solution for SLA-aware federation of cloud, e.g. allowing cloud resources from different providers to be exploited as if they belong to the same cloud. SLAs include QoS as well as some security and privacy attributes (e.g. data location).

7 An Infrastructure-as-a-Service (IaaS) cloud broker mechanism intended to provide cloud users with the requested number of virtual machines from multiple providers with the best cost/performance ratio, in a given price range. This can involve consideration of the

[112] A. Amato, B.D. Martino, and S. Venticinque, "*Cloud brokering as a service*", in3PGCIC, 2013, pp. 9--16.

[113] M. Frtunic, F. Jovanovic, M. Gligorijvic, L. Dordevic, S. Janicijevic, P.H. Meland, K. Bernsmed, and H. N. Castejoen, "*Cloudsurfer - a cloud broker application for security concerns*", in CLOSER, 2013, pp. 199--206.

[114] S.K. Garg, S. Venugopal, and R. Buyya, "*A meta-scheduler with auction based resource allocation for global grids*", in ICPADS, IEEE, 2008, pp. 187--194.

[115] R. Buyya, S. Pandey, and C. Vecchiola, "*Cloudbustoolkit for market-oriented cloud computing*", in Proceedings of the 1st International Conference on Cloud Computing, ser. CloudCom '09, Berlin, Heidelberg: Springer-Verlag, 2009, pp. 24--44

[116] Aniketos Project: http://www.aniketos.eu

[117] A. Amato and S. Venticinque, "*Multi-objective decision support for brokering of cloud SLA*", in Proceedings of the 2013 27thInternationalConference on Advanced Information Networking and Applications Workshops, Washington, DC, USA: IEEE Computer Society, 2013, pp. 1241--1246.

[118] A. Amato, G. Cretella, B. DiMartino, and S. Venticinque, "*Semantic and agent technologies for cloud vendor agnostic resource brokering*", in Proceedings of the 2013 27th International Conference on Advanced Information Networking and Applications Workshops, Washington, DC, USA: IEEE Computer Society,2013, pp. 1253--1258.

[119] A. A. Gaivoronski, D. Strasunskas, P. J. Nesse, and S. Svaet, "*Beyond best effort: Choosing connectivity portfolio for cloud brokering platform by risk/profit trade-off*", in International Teletraffic Congress, 2013, pp. 1--9.

[120] SLA@SOI: http://sla-at-soi.eu

[121] S. K. Nair, S. Porwal, T. Dimitrakos, A. J. Ferrer, J. Tordsson, T. Sharif, C. Sheridan, M. Rajarajan, and A.U. Khan, "*Towards secure cloud bursting, brokerage and aggregatio*n", in Proceedings of the 2010 Eighth IEEE European Conference on Web Service, Washington, DC, USA: IEEE Computer Society, 2010, pp.189--196.

[122] Contrail project: http://www.contrail-project.eu

heterogeneity of cloud providers that have different infrastructures and privacy policies within a cloud brokering approach.[123]

8 Brokerage for cross-cloud federation.[124] [125] [126]

9 Reputation frameworks for determining trustworthiness and assisting partner discovery, as part of a cloud brokering approach. [127] [128] [129] [130]

10 User interfaces [131] and requirements analysis [132]

The main differentiation between this body of research and our Cloud Offerings Advisory Tool (COAT) is the focus of the latter on elucidation, explanation and comparison of privacy and security-related non-functional requirements that are reflected in different cloud service offerings. We do not utilize automated contract specification languages, nor new algorithms to rank the results in an "optimal" manner (though we push results that have strong encryption to the top), as considered within the prior work listed above, although those approaches could be integrated as an extension of our approach if desired. Similarly, our approach could be extended to provide transparency about non-functional requirements in a broader sense than just privacy-related ones. The choice made was a practical one, motivated by the project focus, the state of the market in terms of contractual representation and legal considerations, as explained in this deliverable.

5.3 Scope of the tool

Current cloud brokers focus on finding matches (proper cloud services) based on functional requirements (i.e. Price, Service Type) rather than security and data protection requirements. The lack of a standardized machine-readable contract language that can be used for automatic discovery, negotiation, and reasoning presents a big challenge for such services. Based on this lack of focus on security and data protection requirements in brokerage tools, we have developed a tool called Cloud Offerings Advisory Tool (COAT) to filter the variety of offers being presented to the user based on these security and data protection attributes. The tool acts as an independent web-based broker that:

- checks and gathers user requirements (some functional and mostly security and data protection requirements as explained further in this section),
- matches offers by cloud service providers,
- compares these offers,

[123] J. Tordsson, R. S. Montero, R. Moreno-Vozmediano, and I. M. Llorente, “*Cloudbrokering mechanisms for optimized placement of virtual machines across multiple providers*”, Future General Computer System, vol.28, no.2, pp.358--367, Feb. 2012.

[124] D. Bernstein and Y. Demchenko, “*The ieee intercloud testbed -- creating the global cloud of clouds*”, in Proceedings of the 2013 IEEE International on Cloud Computing Technology and Science - Volume 02, ser. CLOUDCOM '13, Washington, DC, USA: IEEE Computer Society, 2013, pp. 45-50.

[125] J. B. Abdo, J. Demerjian, H. Chaouchi, K. Barbar, and G. Pujolle, “*Broker-based cross-cloud federation manager*”, in ICITST, 2013, pp. 244--251.

[126] E. Badidi, "*A cloud service broker for SLA-based SaaS provisioning*", in International Conference on Information Society (i-Society 2013), Toronto, Canada, 2013, pp. 61--66.

[127] J. Abawajy, “*Determining service trustworthiness in intercloud computing environments*”, Parallel Architectures, Algorithms, and Networks, International Symposium on, vol.0, pp. 784--788, 2009.

[128] S.M. Habib, S. Hauke, S. Ries, and M. Muehlhaueser, “*Trust as a facilitator in cloud computing: a survey*”, Journal of Cloud Computing: Advances, Systems and Applications, vol.1, p.33, Aug. 2012, provisional version.

[129] A. Norta and L. Kutvonen, “*A cloud hub for brokering business processes as a service: A platform that supports semi-automated background checked partner discovery for cross-enterprise collaboration*”, Annual SRII Global Conference, vol.0, pp. 293--302, 2012.

[130] P. Khanna and B. Babu, “*Cloud computing brokering service: A trust framework*”, in CLOUD COMPUTING 2012, IARIA.

[131] J. Lee, J. Kim, D.-J. Kang, N. Kim, and S. Jung, “*Cloud service broker portal: Main entry point for multi-cloud service providers and consumers*”, in Advanced Communication Technology (ICACT2014).

[132] K. Zachos, J. Lockerbie, B. Hughes, and P. Matthews, “*Towards a framework for describing cloud service characteristics for use by chief information officers*”, in RESS. IEEE, 2011, pp. 16--23.

- explains the terms of offerings,
- suggests best offerings that match the user requirement,
- and gives general guidance to users on service offerings.

As part of best accountability practices promoted by our project, the tool educates the user on the meaning of the requirements/attributes and offers guidance on understanding the contractual terms in these offers.

To understand the security and data protection requirements to be addressed in the tool, we explored iteratively the attributes/areas of interest to be covered by COAT. First, we looked into the contracts publicly available online as, for instance, Dropbox[133], Wuala[134], JottaCloud[135], TeamDrive[136]. Second, we identified particular areas of interest in the light of the Data Protection Directive and the proposed Data Protection Regulation[137]. Finally, we did an extended filtering of the attributes on the basis of the finding of the "Survey of the standard contracts and SLAs'' aiming at the creation of a questionnaire accessible to the intended users of the tool, SMEs and end-users searching for certain cloud services. The result of these analysis was the attributes identified in Section 3.

5.4 Tool description

Several contractual terms of a number of cloud storage services were initially assessed against a list of important contractual attributes that users consider (or should ideally consider) when choosing a service. Naturally, terms and conditions of cloud products tend to address the same attributes in different manners. For instance, an important contractual attribute is with regards to the issue of data transfer – a particular user may not want to have her data transferred anywhere outside of the EU – yet whether or not data can be transferred outside of the EU for a particular service depends on the cloud provider's terms about transfer of data. The services initially assessed, however, offered mostly Software as a Service. Other cloud services, constituting the remaining service models – PaaS and IaaS – were then considered in order to determine whether different types of services determine which attributes are most relevant to consider when choosing cloud services, and to what extent the service model considered influences the elements of the cloud contracts taken into account. As of now, it seems that the service model classification, albeit useful for other, descriptive purposes, offers but a feeble guidance in developing a framework for cloud contracting, when compared with other characteristics that differentiate cloud offerings between each other – whether the service is free or has to be paid for or the CSPs principal place of business being prime examples of this. Although, the standard contracts available online primarily relate to the offering of SaaS services, the data protection related attributes incorporated in the tool's questionnaire remain valid for other service delivery models as well.

Given the state of the market discussed earlier, the need for a tool to address specific users' non-functional requirements, and based on the analysis under Section 3 on standard contracts, we developed the Cloud *Offerings Advisory Tool* to act as a matchmaker (matching these user requirements with appropriate cloud service offerings) and provide information/guidance to potential cloud customers- Small and Medium Enterprises (SMEs) and data subjects/end-users- on: how to understand and assess what a cloud service provider is offering from a privacy and security perspective, how to compare offerings (from a data protection compliance and provider accountability point of view), and to offer guidance on the meaning of the comparison attributes. The output is a guided comparison of the service offers along with an explanation of potential risks. The tool also logs the offered advice -in the case of an SME user- and the user's decision for accountability purposes.

[133] Dropbox: http://www.dropbox.com

[134] Wuala: http://www.wuala.com

[135] JottaCloud: http://www.jottacloud.com

[136] TeamDrive: http://www.teamdrive.com

[137] European Commission, "Proposal for a Regulation of the European Parliament and of The Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)" COM 2012 (011) final

The tool is an independent web-based matchmaker that is unique in how it focuses on the security and privacy requirements given by the user to find appropriate service offerings matching these requirements and how it give guidance to the user.

Note that *the term cloud customer* refers to an entity that maintains a business relationship with and uses services from a cloud provider. *Cloud provider* refers to an entity responsible for making a service available to cloud customers[138]. The NIST cloud computing reference architecture describes the role of a cloud broker [139]"*an entity that manages the use, performance and delivery of cloud service and negotiates relationships between Cloud Providers and Cloud Consumers*". We add to this definition that a cloud broker should be able to match offers to users' needs as well.

Figure 1 illustrates a simplified version of the process data flow. We explain the development of the tool in the next subsections by first introducing its interface and data flow, and then discussing the COAT components, architecture and implementation details.

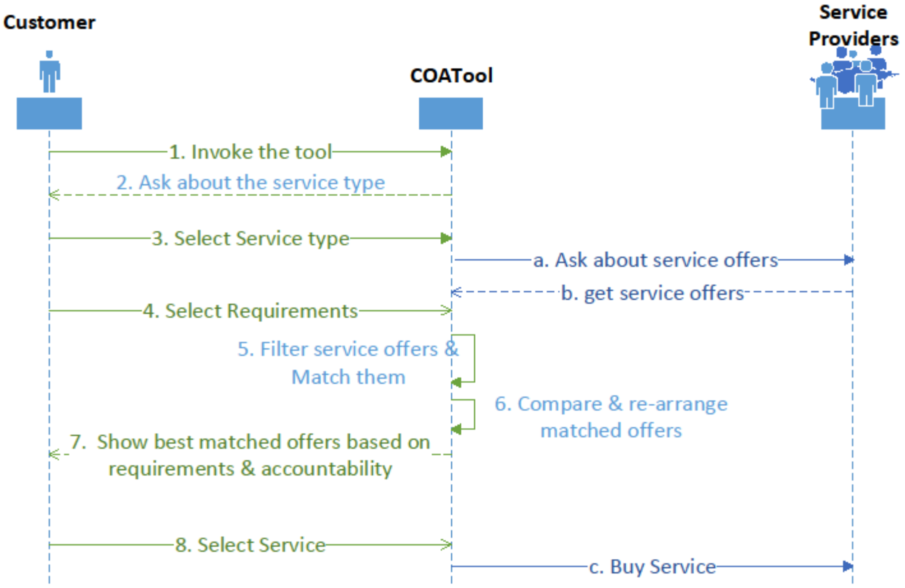

Customer
COATool
Service Providers
1. Invoke the tool
2. Ask about the service type
3. Select Service type
a. Ask about service offers
b. get service offers
4. Select Requirements
5. Filter service offers & Match them
6. Compare & re-arrange matched offers
7. Show best matched offers based on requirements & accountability
8. Select Service
c. Buy Service

Figure 1: COAT Process Data Flow

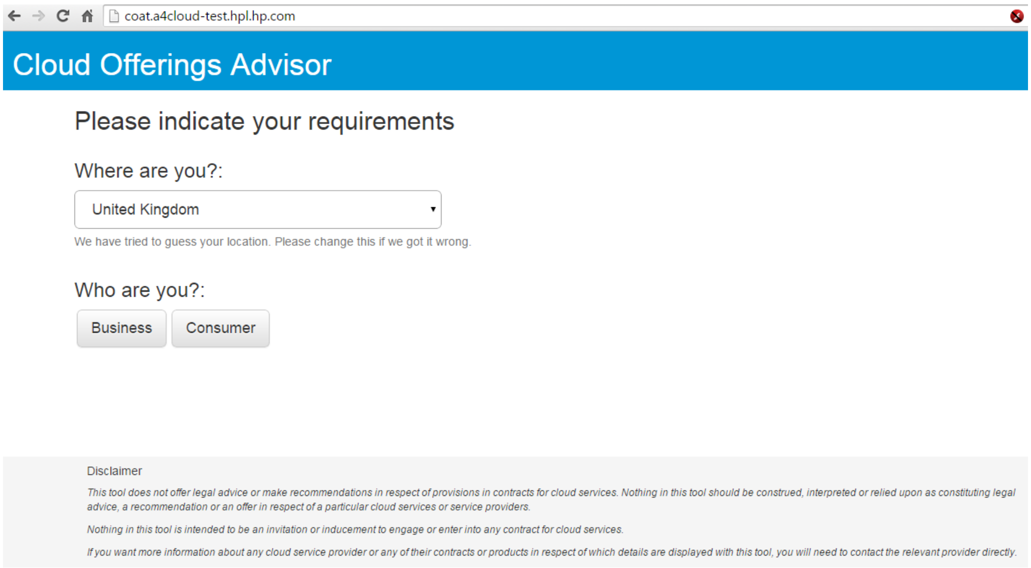
User Interface and Data Flow

COAT is a web-based tool. The landing page asks the user about a) their location (anticipates it first based on the IP address) and b) their role (whether they are a business SME or an end-user) as shown in Figure 2.The tool proceeds by asking the user about the type of service they are searching for, shown in Figure 3 (for SME) and Figure 4 (for end-user). The tool then uses dynamic filtering:

- after selecting the service type. It shows the users the initial list of service offerings filtered only by the type of service they offer.
- during filling/answering the requirements questionnaire the list is updated after answering each requirement, filtering the service offerings based on the values of these answers.

[138] A detailed description of all cloud roles can be found in Dziminski et al., ''*Report detailing conceptual framework",* Cloud Accountability Project, D:C-2.1, (2014).

[139]R.B. Bohn, J. Messina, F. Liu, J. Tong, and J. Mao, ``NIST cloud computing reference architecture.'' in SERVICES, 2011, pp. 594--596.



coat.a4cloud-test.hpl.hp.com

Cloud Offerings Advisor

Please indicate your requirements

Where are you?:

United Kingdom

We have tried to guess your location. Please change this if we got it wrong.

Who are you?:

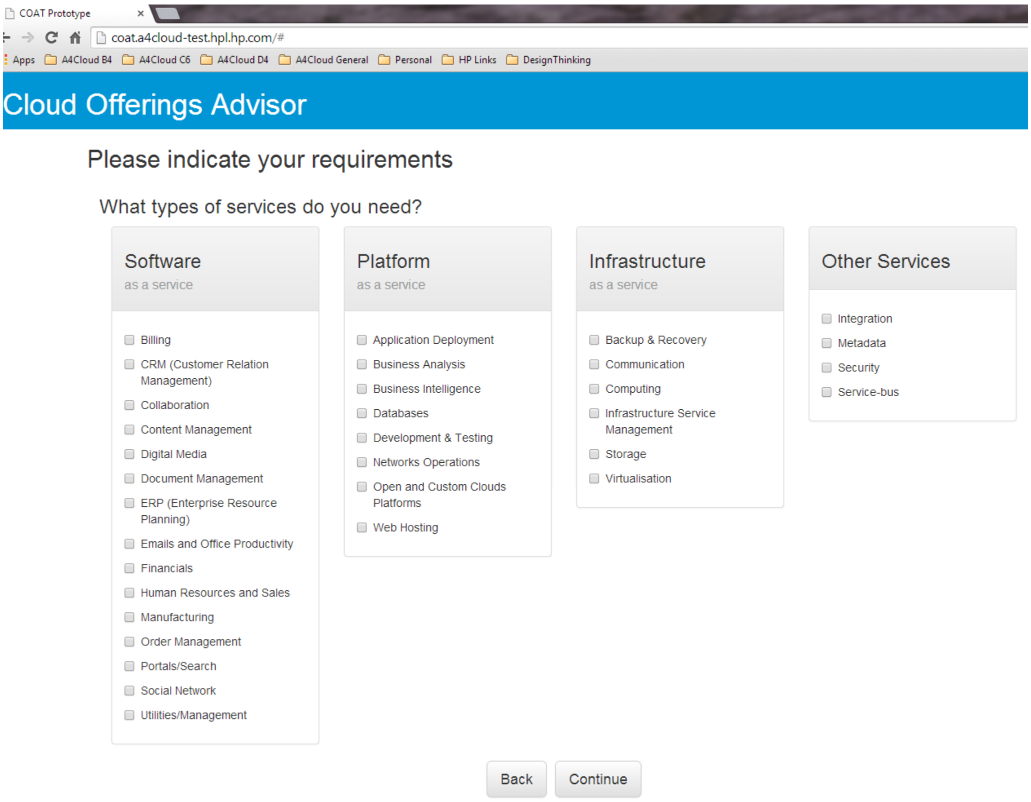
Disclaimer

This tool does not offer legal advice or make recommendations in respect of provisions in contracts for cloud services. Nothing in this tool should be construed, interpreted or relied upon as constituting legal advice, a recommendation or an offer in respect of a particular cloud services or service providers.

Nothing in this tool is intended to be an invitation or inducement to engage or enter into any contract for cloud services.

If you want more information about any cloud service provider or any of their contracts or products in respect of which details are displayed with this tool, you will need to contact the relevant provider directly.

Figure 2: COAT Landing Page



coat.a4cloud-test.hpl.hp.com/#

Cloud Offerings Advisor

Please indicate your requirements

What types of services do you need?

Software
as a service

- □ Billing
- □ CRM (Customer Relation Management)
- □ Collaboration
- □ Content Management
- □ Digital Media
- □ Document Management
- □ ERP (Enterprise Resource Planning)
- □ Emails and Office Productivity
- □ Financials
- □ Human Resources and Sales
- □ Manufacturing
- □ Order Management
- □ Portals/Search
- □ Social Network
- □ Utilities/Management

Platform
as a service

- □ Application Deployment
- □ Business Analysis
- □ Business Intelligence
- □ Databases
- □ Development & Testing
- □ Networks Operations
- □ Open and Custom Clouds Platforms
- □ Web Hosting

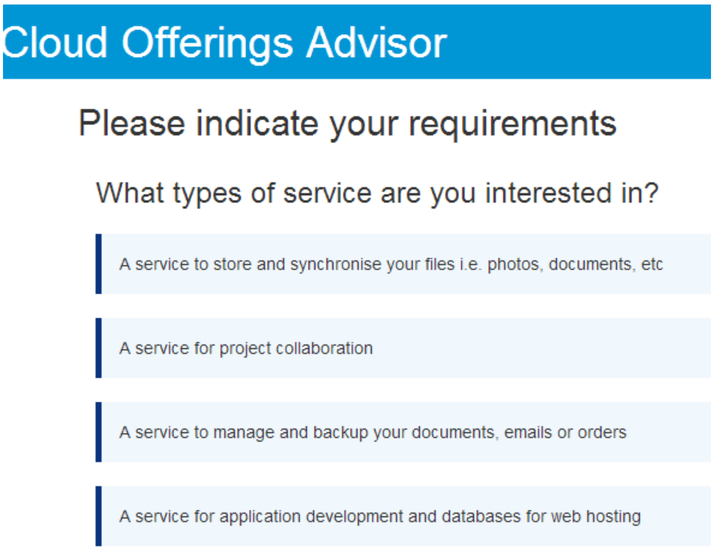
Infrastructure
as a service

- □ Backup & Recovery
- □ Communication
- □ Computing
- □ Infrastructure Service Management
- □ Storage
- □ Virtualisation

Other Services

- □ Integration
- □ Metadata
- □ Security
- □ Service-bus

Figure 3: Service Type Question shown to SME



Cloud Offerings Advisor

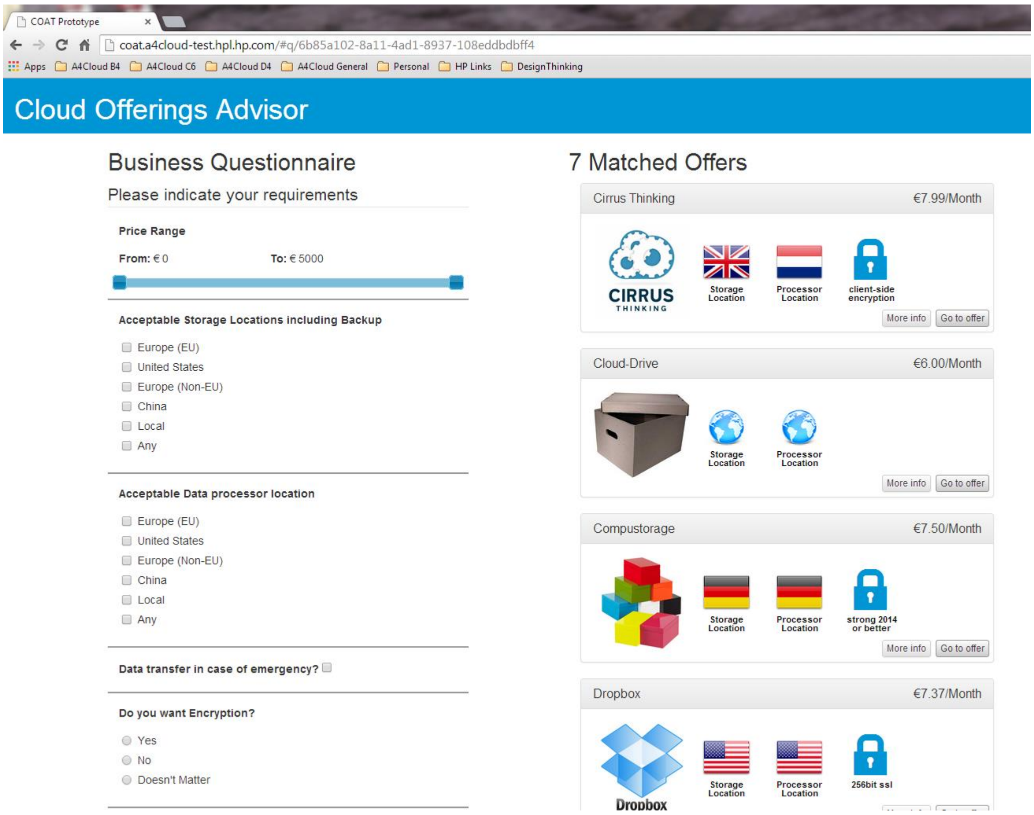
Please indicate your requirements

What types of service are you interested in?

- A service to store and synchronise your files i.e. photos, documents, etc
- A service for project collaboration
- A service to manage and backup your documents, emails or orders
- A service for application development and databases for web hosting

Figure 4: COAT Service Type Question show to end users

Figure 5 and Figure 6 are some snapshots of the tool. They show what the user sees once the service type is selected and the requirements/attributes options displayed to him to select from. The user does not have to indicate all of his requirements to have a list of offers. Dynamic filtering works every time the user selects an answer to limit the resulting list of offers (matching his requirements).
Figure 7 shows how the tool explains to the user the meaning of an attribute/requirement.



Cloud Offerings Advisor

Business Questionnaire

Please indicate your requirements

Price Range

From: € 0 **To:** € 5000

Acceptable Storage Locations including Backup

□ Europe (EU)
□ United States
□ Europe (Non-EU)
□ China
□ Local
□ Any

Acceptable Data processor location

□ Europe (EU)
□ United States
□ Europe (Non-EU)
□ China
□ Local
□ Any

Data transfer in case of emergency? □

Do you want Encryption?

○ Yes
○ No
○ Doesn't Matter

7 Matched Offers

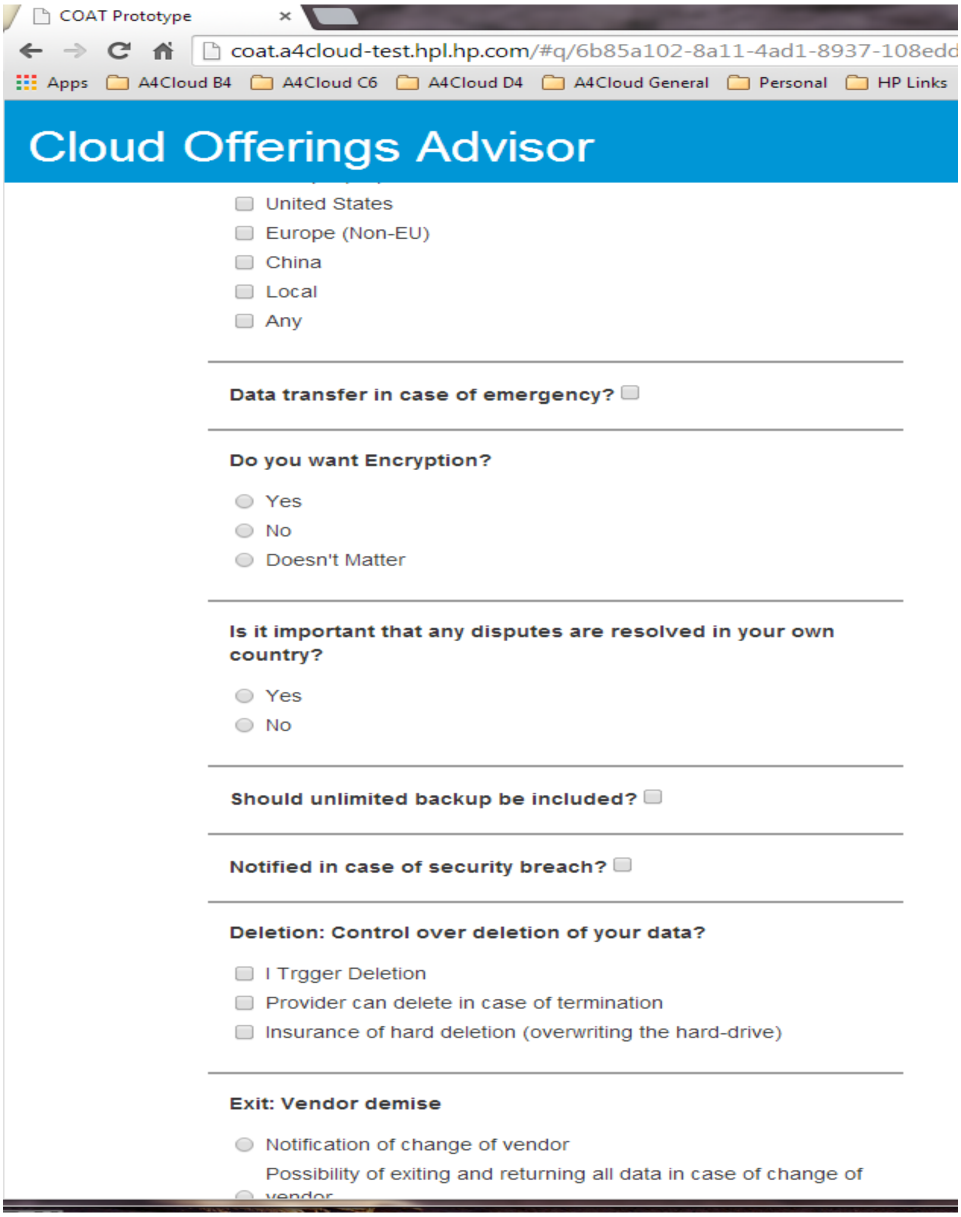
Cirrus Thinking €7.99/Month

Cloud-Drive €6.00/Month

Compustorage €7.50/Month

Dropbox €7.37/Month

Figure 5: COAT Interface



Cloud Offerings Advisor

□ United States
□ Europe (Non-EU)
□ China
□ Local
□ Any

Data transfer in case of emergency? □

Do you want Encryption?

○ Yes
○ No
○ Doesn't Matter

Is it important that any disputes are resolved in your own country?

○ Yes
○ No

Should unlimited backup be included? □

Notified in case of security breach? □

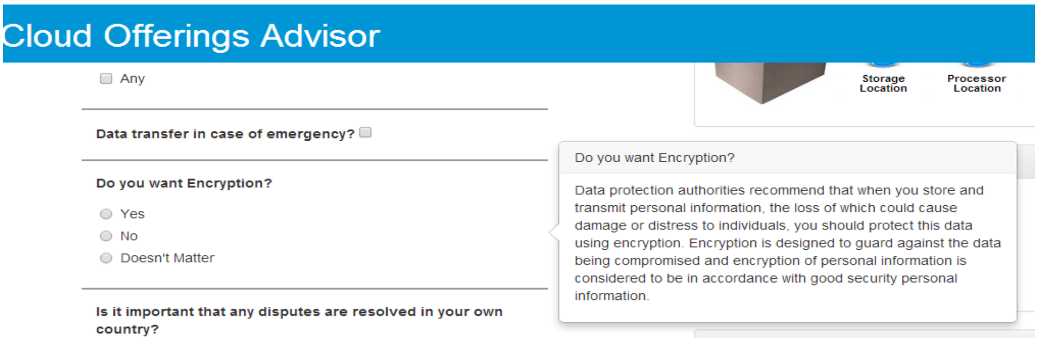
Deletion: Control over deletion of your data?

□ I Trgger Deletion
□ Provider can delete in case of termination
□ Insurance of hard deletion (overwriting the hard-drive)

Exit: Vendor demise

○ Notification of change of vendor
○ Possibility of exiting and returning all data in case of change of vendor

Figure 6: Some of the requirements shown to the user



Cloud Offerings Advisor

□ Any

Data transfer in case of emergency? □

Do you want Encryption?

○ Yes
○ No
○ Doesn't Matter

Is it important that any disputes are resolved in your own country?

Do you want Encryption?

Data protection authorities recommend that when you store and transmit personal information, the loss of which could cause damage or distress to individuals, you should protect this data using encryption. Encryption is designed to guard against the data being compromised and encryption of personal information is considered to be in accordance with good security personal information.

Figure 7: Explanation Text for each attribute

5.5 Architecture and implementation

In this section we explain the main components of the tool and how it was implemented.

The inputs to the tool are:

- User information (location and role)
- User needs and requirements (answers to the requirement questionnaire)
- Structured service offerings (contract details)
- A model of cloud contracts and points of attention

The outputs are:

- Matching results of service offerings
- Guidance on things to pay attention to when exploring and comparing the terms of service offerings
- Overview of comparable service offerings along with links to their contract details (organized by attributes to facilitate easy understanding of contract terms)
- A requirement list to give to the Cloud Service Provider (CSP)
- SME guidance

The main internal processes are:

- Matching offers to requirements
- Assessment of a cloud service provider offering from a privacy and security perspective
- Comparison of offerings (from a data protection compliance and provider accountability point of view)
- Guidance on the meaning of the comparison attributes and education of users on security
- Logging of the offered advice and the user's decision

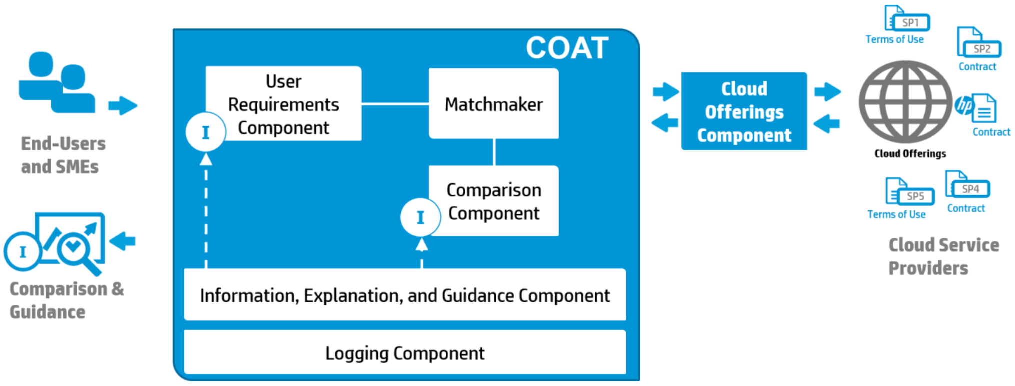


Figure 8: COAT Components

The main components of the tool are the (see Figure 8):

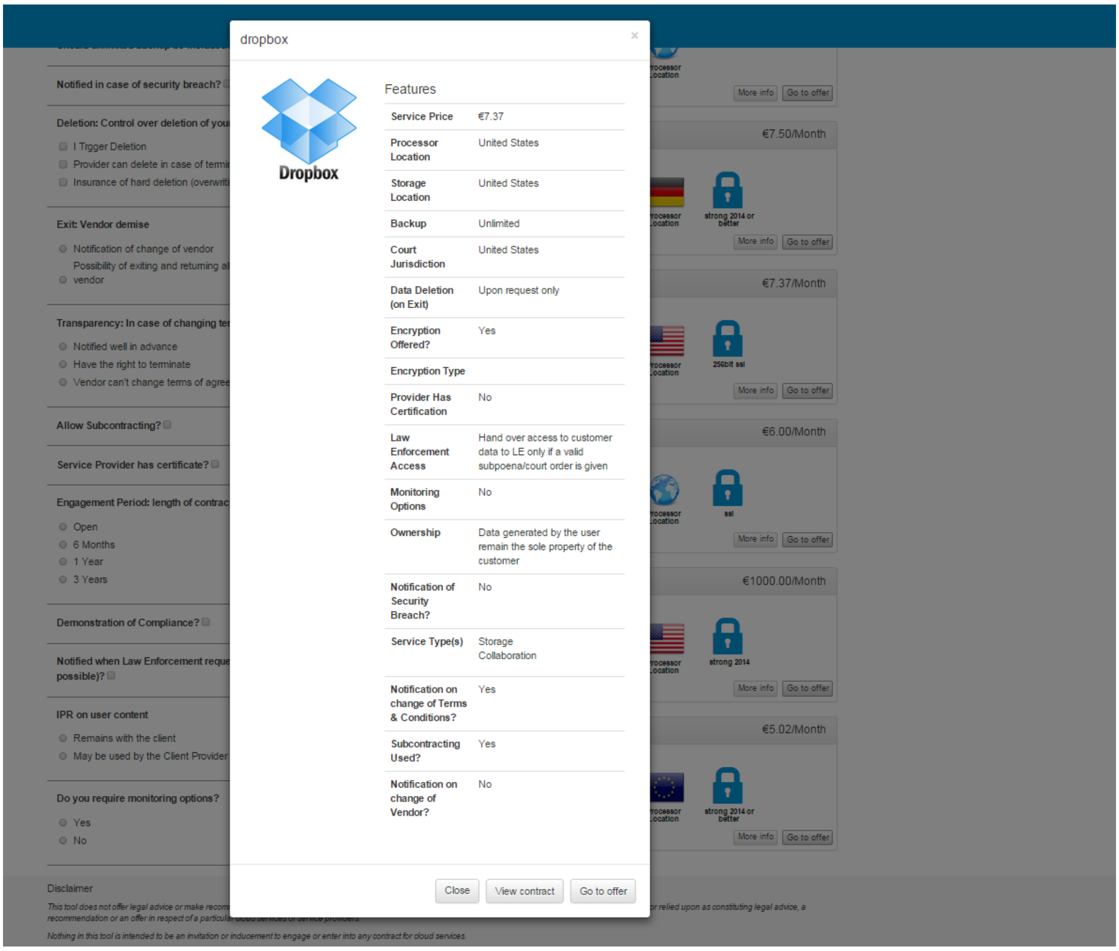
User Requirement Component. Based on a pre-defined set of requirements (attributes analysed by the project as discussed in Section3), the tool asks the user -in the form of an easy-to-use questionnaire- to enter his/her requirements or what (s)he is searching for. Starting by asking about the type of service (s)he wants (see Figure 3 and Figure 4), then moving to attributes like price, type of encryption, location of the service, notifications, etc. Some examples of the requirements questionnaire are shown in Figure 5, Figure 6 and Figure 7. The questionnaire is dynamic; some answers triggers additional questions. For example, if the answer to the "*Do you want Encryption?*" question is yes, an additional question of *"What type of Encryption?"* appears.

Matchmaker Component. After gathering user requirements, the User Requirement Component passes a list of the user's answers to the matchmaker which in return matches the values of these attributes to the values of the same attributes in the service offerings database. The resulting list of matches is then passed to the Comparison Component.

Comparison Component. After getting the list of matched service offerings, this component re-arranges the list of matches based on "exact matches" and "most secure matches". While we don't employ a complicated ranking algorithm for the service offerings rankings, we still push the service offerings with strong encryption options to the top of the list the user sees. This way the user has an easy access to the more secure option. The resulting list is a combination of exact matching list and close matching list with only some of the values being matched. Further future work and research on the ranking of the offers is explained in section 6.

Information and Guidance Component. For each requirement and question asked to the user, a helping text is provided to explain not only the meaning of the question but also the importance of such a requirement (see Figure 8). This component feeds the explanation-text to the interface to help a user in understanding the requirements and also the terms of the contracts in the service offerings. On the list of matched offers, clicking on "*View Contract*" takes the user to a new page which shows a structured explanation of the service contract (example in Figure 9).

Logging Component. This component logs the values of the requirements questionnaire and the user's selection from the list of service offerings. This is done for accountability purposes.



Notified in case of security breach? □

Deletion: Control over deletion of you

□ I Trgger Deletion
□ Provider can delete in case of termi
□ Insurance of hard deletion (overwrit

Exit: Vendor demise

○ Notification of change of vendor
○ Possibility of exiting and returning al vendor

Transparency: In case of changing te

○ Notified well in advance
○ Have the right to terminate
○ Vendor can't change terms of agree

Allow Subcontracting? □

Service Provider has certificate? □

Engagement Period: length of contrac

○ Open
○ 6 Months
○ 1 Year
○ 3 Years

Demonstration of Compliance? □

Notified when Law Enforcement reque possible)? □

IPR on user content

○ Remains with the client
○ May be used by the Client Provider

Do you require monitoring options?

○ Yes
○ No

dropbox ×

Features

Service Price	€7.37
Processor Location	United States
Storage Location	United States
Backup	Unlimited
Court Jurisdiction	United States
Data Deletion (on Exit)	Upon request only
Encryption Offered?	Yes
Encryption Type	
Provider Has Certification	No
Law Enforcement Access	Hand over access to customer data to LE only if a valid subpoena/court order is given
Monitoring Options	No
Ownership	Data generated by the user remain the sole property of the customer
Notification of Security Breach?	No
Service Type(s)	Storage Collaboration
Notification on change of Terms & Conditions?	Yes
Subcontracting Used?	Yes
Notification on change of Vendor?	No

Close | View contract | Go to offer

rocessor Location

More info | Go to offer

€7.50/Month

rocessor Location | strong 2014 or better

More info | Go to offer

€7.37/Month

rocessor Location | 256bit ssl

More info | Go to offer

€6.00/Month

rocessor Location | ssl

More info | Go to offer

€1000.00/Month

rocessor Location | strong 2014

More info | Go to offer

€5.02/Month

rocessor Location | strong 2014 or better

More info | Go to offer

Disclaimer

This tool does not offer legal advice or make recom… or relied upon as constituting legal advice, a recommendation or an offer in respect of a particul… cloud services or service providers.

Nothing in this tool is intended to be an invitation or inducement to engage or enter into any contract for cloud services.

Figure 9: COAT Example of an Offer Details

Figure 10 shows details about COAT implementation. The tool is a web-based tool connecting to a database of predefined questions regarding the user's requirements and a database of service offerings (MySQL[140]).

The *server-side application* and the *web service layer* that provide access to the questionnaire management and matchmaker are written in Java. The *Matchmaker component* along with the *Questionnaire management* (logic) are implemented in Java as well. The *client-side application* is implemented using HTML5 and JavaScript and is backed by Backbone[141] for a client-side MVC structure.

The offers management and associated web services are written in Python[142]. The Search Index used in finding the matched service offerings is done by SOLR. We use RESTful API as a transport layer and JSON[143] as the data-interchange format.

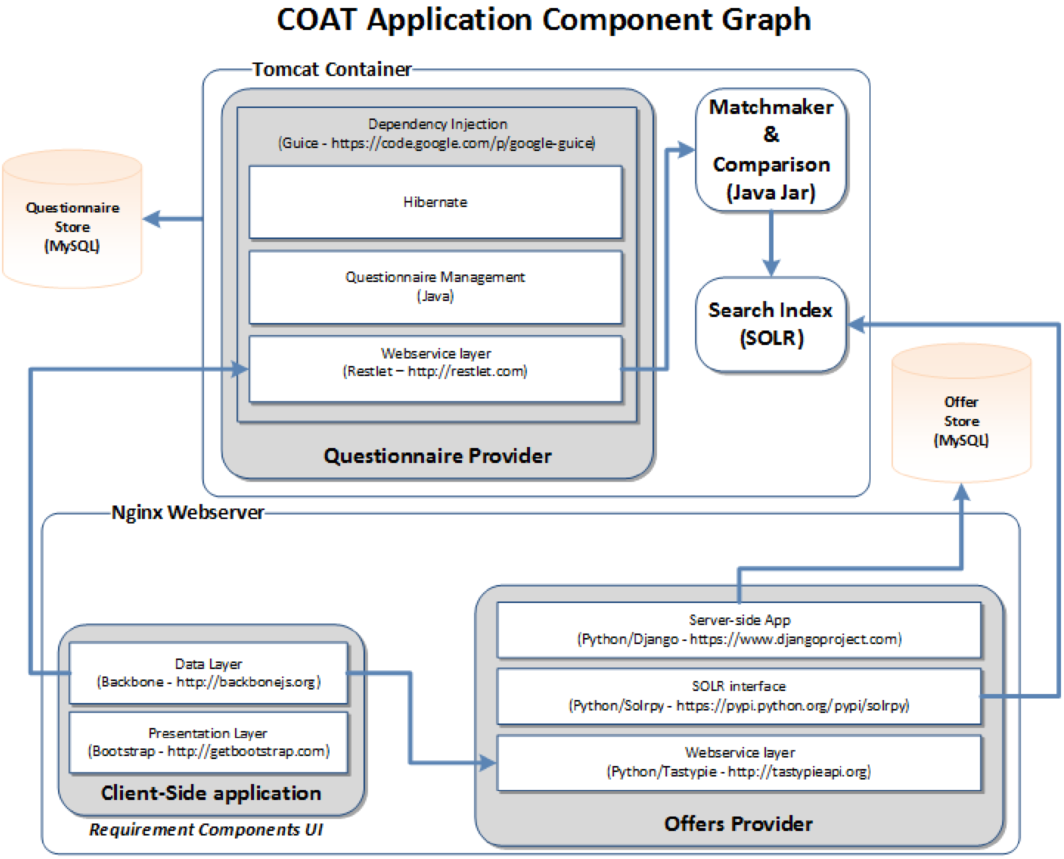

COAT Application Component Graph
Tomcat Container
Dependency Injection
(Guice - https://code.google.com/p/google-guice)
Hibernate
Questionnaire Management
(Java)
Webservice layer
(Restlet – http://restlet.com)
Questionnaire Provider
Matchmaker
&
Comparison
(Java Jar)
Search Index
(SOLR)
Questionnaire
Store
(MySQL)
Offer
Store
(MySQL)
Nginx Webserver
Data Layer
(Backbone - http://backbonejs.org)
Presentation Layer
(Bootstrap - http://getbootstrap.com)
Client-Side application
Requirement Components UI
Server-side App
(Python/Django - https://www.djangoproject.com)
SOLR interface
(Python/Solrpy - https://pypi.python.org/pypi/solrpy)
Webservice layer
(Python/Tastypie - http://tastypieapi.org)
Offers Provider

Figure 10: COAT's Implementation.

5.6 Testing and feedback

In order to test the tool and as part of our project's dissemination process, we organized two workshops: one for cloud providers and another for cloud customers.

[140] MySQL Source database: http://www.mysql.com/
[141] Backbone: http://backbonejs.org/
[142] Python Programming Language: https://www.python.org
[143] JSON: http://json.org/

In the first workshop ("Cloud of Clouds – Made in Europe, Secured Locally", HP Paris, 16th of June 2014) we invited various cloud providers along with IT cloud professionals. The workshop was attended by 41 participants representing 22 different stakeholders among service providers, independent software/system vendors, university/research and public administration/government. The stakeholders attending the workshop were mostly service providers but also with participants from other relevant groups. The attendees were presented with the purpose of our project and COAT and were engaged in round table discussions to get their feedback. Most of the attendees acknowledged the need for such a tool to match offers based on non-functional requirements especially security and privacy requirements.

Several issues were pointed out during the first workshop. One of the most valuable points raised during this workshop was that unlike SME users, non-expert end users will not like the page that asks about the service types shown in Figure 3. Based on this feedback we have developed two different service-types pages: one for an SME user (Figure 3) with more detailed service-types and one for the non-expert end user which is more user-friendly with less detailed service-types (Figure 4). Another issue raised related to the concern that certain cloud service providers might not cooperate in entering their contract details in the tool service-offerings side (populating the tool with offers). However, our argument is that the tool provides good exposure for them and more specifically an exposure to the unique capabilities and terms that they can offer to their users; this would give small(er) businesses a competitive advantage over large cloud service providers. As part of our future work, the tool will acquire this information automatically.

Note that in the context of the first workshop there was a question on how much the user should know before using the tool. We assume that SME users will know more details about their functional and non-functional requirements than a normal non-expert user. This is why the tool has two sets of requirements questionnaire where the one for the non-expert user is more simplified. Also, most requirements questions are optional giving the user the opportunity to still get results even if he does not know the answers to all questions. The overall feedback was positive and gave us information on how to enhance the tool in the future.

As to the second workshop mentioned previously, it took place on the 20th of June, 2014, in SINTEF Research Center, Norway. The 11 attendees (cloud customers) were asked to give feedback on the tool concept, usage, and to give suggestions on enhancing the tool. The feedback received can be summarized as follows:

- The tool is not complex to understand its purpose and it is easy to use and to be learned quickly.
- The tool functionalities are useful and most attendees had no suggestions to add to them.
- Some attendees suggested the inclusion of a strong reputation system to rate service providers and a way to see the history of the providers.

Also, the attendants of the workshop stressed out that the tool needs to clarify its uniqueness over other brokering tools. Specifically, it should advertise the fact that it focuses on security and privacy requirements and it also provides help for ordinary users to understand contractual terms in a simplified way. Given that the above mentioned workshops took place at an early stage of the present research, the feedback collected provided useful input while developing the tool and adjusting some user interaction parts.

In addition to the formal workshops provided by the project’s Description of Work (DOW), project partners ran an experiment with COAT demo involving end-users and SMEs. The interviewees provided comments both on specific questions and on the overall demo. The most valuable points raised with respect to that stage of development of COAT concerned the completion of the tool’s questionnaire, which was perceived as a burdensome activity rather than as a means that enables them to concretize their requirements and, eventually, help them decide on the appropriate cloud offering. The internal report compiled is annexed at the end of this deliverable.

5.7 The role of an Accountability Maturity Model (AMM)

As the number of offerings in COAT's database grows, the ordering in which the offerings are displayed on the right hand side of the user interface (as the result of the matchmaking process) becomes increasingly significant. The way in which this is done influences the trust relationships and business model. In most cases it would be advantageous for this selection process to be seen to be independent of any favouritism on behalf of the broker operator. One option would be to base the ordering on price. Another would be to integrate with a reputation management system, in which users can rate the cloud service providers. Another would be to use an algorithm developed by one of the research projects cited above (see section 5.1). We are investigating an alternative way of ordering the offerings, in which the accountability of the cloud service provider is used as the determining factor. This is work in progress and a short description of our approach is given below[144]. Hybrid options are also possible, whereby users can choose the mechanism by which the cloud service providers are ranked.

Our current activity centres around a full analysis of the Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM) framework reflecting cloud security controls, in relation to accountability. We have established a relationship between functions / controls of our accountability framework (as described in WP D.2) and the CCM controls, and have then analysed CCM controls as subjects of accountability (i.e. the process of accounting for CCM controls), so that we are able to identify a list of accountability controls that reflect a wider context/standardised approach and can be used as the basis for measurement. Such measurement may involve our accountability metrics (developed within WP C5), or may involve a simpler, more Boolean type of assessment. By aggregating these measurements in a pre-defined way we are able to obtain an overall value that can be used within COAT in order to reflect the output, as explained above.

[144] The current findings of relevant project research are discussed under D:D-2.3: "*Initial reference architecture*", A4Cloud project deliverable, eds. Gittler et al., April 2015.

6 Recommendations and conclusions

The analysis provided in this document described the difficulties in decision making for end users and SMEs intending to use a cloud offered service tailored to their data protection related needs and preferences. These difficulties result mainly from the lack of transparency of cloud computing agreements and the increasing number of CSPs in the market. To mitigate these difficulties and help customers make informed choices, we developed the Cloud Offerings Advisory Tool (COAT).

COAT benefits cloud customers in multiple ways. In particular, the tool allows for an easy comparison between numerous cloud offerings based on user requirements, while using a 'familiar' store interface to reduce complexity of selecting cloud offerings. Moreover, COAT informs cloud customers of the consequences of their choices through the pop texts providing explanation in simplified language and allowing them to identify -in a quick and efficient manner- which contractual provisions to focus on when deciding for an appropriate CSP. Ultimately, the tool enhances transparency of cloud computing agreements and facilitates decision making, while increasing the overall trust in the cloud.

The tool, however, has certain limitations as well[145]. Given that the Terms of Service of cloud contracts change quite often, the internal repository of the tool should be updated quite often. Moreover, as is the case for other tools produced by the project, COAT does not provide legal advice and cannot fully capture the complexities of legal texts; the selection process of certain attributes of cloud contracts for the creation of the questionnaire, as well as the focus on relevant laws at European level – without taking into account any of the national implementations – forms a clear illustration of the latter point raised.

Furthermore, the analysis of cloud contracts from a privacy and data protection perspective and the exploration of comparison websites, as well as the development of COAT itself revealed areas where CSPs can improve transparency, foster genuine choice and differentiate themselves from others. Based on these findings, we recommend that the:

1. The cloud provider should offer a choice of law that relates to the place of residence or business address of the customer.

2. The cloud provider should offer a jurisdiction clause that relates to the place of residence or business address of the customer.

3. Arbitration should be offered to cloud customers together with other options for dispute resolution rather imposed on customers for all types of disputes; this is particular relevant, given that -both in Common Law and Civil Law Countries - there is no appeal procedure for arbitration.

4. As far as the variation of terms is concerned, the technique of sending emails to customers about proposed contract changes is probably the best method of alerting customers to contract changes in a way that is accountable. Customers may choose to ignore the email, but at least the onus is on the cloud provider to take action to alert customers to changes and the burden is not on the customer to check the website for contract changes.

5. The cloud service provider should undertake to take the necessary steps to ensure the preservation and integrity of data processed during the term of the contract.

6. As to data retention, it would improve accountability if the cloud service provider: first, gives a clear time period during which data will be preserved at the end of the contract and does not delete it automatically and immediately on termination of the contract; second, undertakes to

[145] Gleeson, Niamh et al. ''*A4Cloud Tool, Liability and Compliance Investigations",* Cloud Accountability Project D-4.12 (2015).

guarantee the easy portability or reversibility of customer data in a structured and widely used format; and, finally, agrees to work with the customer to effectively erase its data from the cloud providers records in cases where customers have particular concerns about fully erasing or destroying certain types of sensitive data.

7. The CPS explicitly states whether it will disclose information to the Law Enforcement Agencies (LEAs) or not. If this is if and only if there is a valid court order, this should be stated explicitly. If there are other circumstances, this should also be stated explicitly. When it reserves discretion to itself to notify LEAs, it should undertake to let the customer know that disclosure has taken place as soon as reasonably practicable.

8. The CSP at least acknowledges explicitly in its terms of service that it will store and transfer data world-wide, given that cloud computing allows for the continuous flow of data worldwide. In this way, the cloud customer will be properly informed and may decide not to enter in such contract in the first place, while having an explicit acknowledgement that it has a right to know when its data has been transferred outside of specific jurisdictions.

9. If the cloud provider is engaged in monitoring customer data, it should include a clause in the contract acknowledging that it is doing so and explaining why. Also, it is recommended that they provide for options as, for instance, monitoring only the metadata but not the content.

10. The CSP should not include sweeping exclusions of warranties in its contracts; the contracts should at least make it clear that these warranties do not affect the customer's rights to remedies. Note that, in general, Civil Codes within Civil Law jurisdictions (eg Dutch Civil Code) prohibit full exclusion of liabilities resulting from intentional damages or gross negligence.

11. CSPs include clauses providing for service credits since it is an efficient way of providing a remedy to customers for service failure. Nevertheless, especially in Common Law Countries (eg, NL), CSPs should make explicit in the contract that the customer maintains –in addition to service credits- the right for remedies; otherwise it might be that the provisioning of service credits deprives the customer this right (eg. Dutch Civil Code).

Other recommendations addressed to CSPs resulting from other sources (e.g. A29WP) are given earlier in the analysis.

Applying the best practices given above through cloud contracts registered in tool’s repository will strengthen the role of a cloud comparison tool such as COAT in enhancing accountability in the cloud.

References

Abawajy, Jemal. "*Determining service trustworthiness in intercloud computing environments*", Pervasive Systems, Algorithms, and Networks (ISPAN), IEEE (2009).

Abdo, Jacques Bou, et al. "*Broker-Based Cross-cloud federation manager*", Internet Technology and Secured Transactions (ICITST), IEEE (2013).

Amato, Alba, and Salvatore Venticinque. "*Multi-objective decision support for brokering of cloud sla*", Advanced Information Networking and Applications Workshops (WAINA), IEEE (2013).

Amato, Alba, Beniamino Di Martino, and Salvatore Venticinque. "Cloud brokering as a service." *P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC),* IEEE (2013).

Amato, Alba, et al. "*Semantic and agent technologies for cloud vendor agnostic resource brokering*", Advanced Information Networking and Applications Workshops (WAINA)*,* IEEE *(*2013).

Badidi, Elarbi. "A *cloud service broker for SLA-based SaaS provisioning*", Information Society (i-Society), IEEE (2013).

Balboni, Paolo, and Francesca Fontana. "*Cloud computing: A guide to evaluate and negotiate cloud service agreements in the light of the actual european legal framework*", Przegląd Prawa Technologii Informacyjnych. ICT Law Review 1 (2013).

Bernstein, David, and Yuri Demchenko. "*The IEEE Intercloud Testbed--Creating the Global Cloud of Clouds*", Cloud Computing Technology and Science (CloudCom)*,* IEEE (2013).

Bishop, Simon, and Mike Walker. "*The economics of EC competition law"*, Sweet & Maxwell, (2010).

Bradshaw, Simon, Christopher Millard, and Ian Walden. "*Contracts for clouds: comparison and analysis of the terms and conditions of cloud computing services*". International Journal of Law and Information Technology 19.3 (2011).

Bradshaw, Simon, Christopher Millard, and Ian Walden. "*The Terms They Are A-Chargin'… Watching Cloud Contracts Take Shape*". Issues in technology Innovation 7 (2011).

Buyya, Rajkumar, Suraj Pandey, and Christian Vecchiola. "*Cloudbus toolkit for market-oriented cloud computing*", Cloud Computing, Springer Berlin Heidelberg, (2009).

Burden, Kit. "*"Cloud bursts": Emerging trends in contracting for Cloud services*", *Computer Law & Security Review* 30.2 (2014).

Carlton, Dennis W., and Jeffrey M. Perloff. "*Modern industrial organization"*. Addison Wesley (2005).

Civic Consulting, "*Consumer market study on the functioning of e-commerce and Internet marketing and selling techniques in the retail of goods*", European Commission (2011).

CNIL, "*Recommendations for companies planning to use Cloud computing services*", (2012).

CompatibleOne, "*CompatibleOne Open Source Broker Architecture Overview*", white paper (2012).

Competition & Markets Authority, "*Private motor insurance market investigation Final report*", CMA (2014).

Dziminski, Brian et al. "*Report detailing conceptual framework*", Cloud Accountability Project D:C-2.1 (2014).

Directorate General for Internal Policies, Policy Department A: Economic And Scientific Policy, “Cloud computing – Study”, IP/A/IMCO/ST/2011 - PE 475.104 (2012)

EIOPA, “*Report on Good Practices on Comparison Websites*”, EIOPA-CCPFI-13/100 (2014).

European Commission, “*Comparison Tools – Report from the Multi-Stakeholder Dialogue. Providing consumers with transparent and reliable information*”, European Consumer Summit (2013).

European Commission, "*Unleashing the Potential of Cloud Computing in Europe*”, Commission Staff Working Document SWD (2012) 271 final (2012).

f5 Networks inc., “*Integrating the Cloud: Bridges, Brokers and Gateways*”, white paper (2012).

Frtunic, Milena, et al. "*CloudSurfer-A Cloud Broker Application for Security Concerns*", *CLOSER* (2013).

Gaivoronski, Alexei, et al. "*Beyond best effort: Choosing connectivity portfolio for cloud brokering platform by risk/profit tradeoff*", Teletraffic Congress (ITC), 2013 25th International, IEEE (2013).

Garg, Saurabh Kumar, Srikumar Venugopal, and Rajkumar Buyya. "A meta-scheduler with auction based resource allocation for global grids." *Parallel and Distributed Systems, ICPADS'08,* IEEE *(*2008).

Gittler, Frederoc et al., “*Initial reference architecture, A4Cloud project deliverable*”, Gittler et al. (eds.), Cloud Accountability Project D:D-2.3 (2015).

Gleeson, Niamh et al. *''A4Cloud Tool, Liability and Compliance Investigations",* Cloud Accountability Project D-4.12 (2015).

Grivas, Stella Gatziu, Tripathi Uttam Kumar, and Holger Wache. "*Cloud broker: Bringing intelligence into the cloud*", Proc. CLOUD2010, IEEE (2010).

Grozev, Nikolay, and Rajkumar Buyya. "Inter-Cloud architectures and application brokering: taxonomy and survey." *Software: Practice and Experience* 44.3 (2014).

Habib, Sheikh Mahbub, et al. "*Trust as a facilitator in cloud computing: a survey*", Journal of Cloud Computing 1.1 (2012).

Hon, W. Kuan, Christopher Millard, and Ian Walden, "*Negotiating Cloud Contracts-Looking at Clouds from Both Sides Now*", 16 STAN. TECH. L. REV. 81, Queen Mary School of Law Legal Studies Research Paper No. 117/2012 (2012).

Hon, Kuan et al. “*White paper on the proposed data protection regulation*”, Cloud Accountability Project D:B-5.1 (2014).

Hustinx, Peter. "*Opinion of the European Data Protection Supervisor on the Commission's Communication on ‘Unleashing the potential of Cloud Computing in Europe’*", European Data Protection Supervisor (2012).

Information Commissioner’s Office, “Personal information online code of practice”, ICO (2010).

International Working Group on Data Protection in Telecommunications. “*Working Paper on Cloud Computing - Privacy and data protection issues - “Sopot Memorandum”*”, 675.44.8 (2012).

Khanna, P., and B. Babu. "*Cloud Computing Brokering Service: A Trust Framework*", *CLOUD COMPUTING* (2012).

Lear, “*Can ‘Fair’ Prices Be Unfair? A Review of Price Relationship Agreements*”, OFT 1438 (2012).

Lear, “*Price Relationship Agreements: Economic Analysis and Implications for Competition*”, Lear Competition Note (2012).

Lee, Jihyun, et al. "*Cloud Service Broker Portal: Main entry point for multi-cloud service providers and consumers*", Advanced Communication Technology (ICACT), IEEE (2014).

Liu, Fang, et al. "*NIST cloud computing reference architecture*", NIST special publication 500 (2011).

Millard, Christopher J., ed. *“Cloud Computing Law*”. Oxford University Press (2013).

Motta, Massimo. “*Competition policy: theory and practice”*. Cambridge University Press (2004).

MSDCT, “*Comparison Tools Report from the Multi-Stakeholder Dialogue - Providing consumers with transparent and reliable information*”, European Consumer Summit (2013).

Nair, Srijith K., et al. "*Towards secure cloud bursting, brokerage and aggregation*" Web Services (ECOWS), IEEE (2010).

Norta, Alex, and Lea Kutvonen. "*A Cloud HUB for Brokering Business Processes as a Service: A" Rendezvous" Platform that Supports Semi-Automated Background Checked Partner Discovery for Cross-Enterprise Collaboration*", SRII Global Conference (SRII), 2012 Annual. IEEE (2012).

Poullet, Yves, et al. "*Cloud Computing and its implications on data protection*", Council of Europe (2010).

Reed, Chris et al. “*Survey of cloud standard contracts and SLAs; evolution in terms of accountability”*”, Neeson et al. (eds.) Cloud Accountability Project D4.2 (2015).

Tordsson, Johan, et al. "*Cloud brokering mechanisms for optimized placement of virtual machines across multiple providers*", Future Generation Computer Systems 28.2 (2012).

Whish, Richard, and David Bailey. “*Competition law”*. Oxford University Press (2012).

Zachos, Konstantinos, et al. "*Towards a framework for describing cloud service characteristics for use by chief information officers*", Requirements Engineering for Systems, Services and Systems-of-Systems (RESS), IEEE (2011).

Appendices

A. Glossary for cloud contracts

The contractual terms and conditions (“T&Cs”) analysed in light of the nuances they assume in a cloud environment were found in several different documents, their placement depending on the provider inconsideration. Despite the differences running between the CSPs analysed, and the fact those T&Cs are written in different styles and with assorted formulations, the documents in which they are to be found can be grouped as follows:

Acceptable Use Policy (AUP):
The AUP forbids certain activities which are not in line with the purposes that the cloud service is meant to be used for.

Privacy Policy:
This document explains how the provider uses and protects the user’s personal data. The personal data may be related directly to individuals acting in their capacity as cloud customers or indirectly related to data subjects, for example where cloud customers are businesses using the services to process information about their employees or customers. Since one policy is usually used for all services and products, this document is presented separately from the Terms of Service.

Service Level Agreement (SLA):
This can be within the Terms of Service but is more usually presented as a separate document. It relates to the way the service works, responsibilities of the provider, rights of users relating to the service, compensation etc. This document is associated with paid services and commercial cloud agreements.

Negotiated terms:
Cloud contracts can be negotiated as well, usually where certain cloud customers require specific arrangements and providers deem that the strategic or financial value of a commercial arrangement requires special treatment. Such deals typically involve corporate or government entities as customers and they most commonly negotiated liability, privacy and data security provisions. The starting point of the negotiated contract's drafting remains set by the CSPs – that is, the basis from which the negotiation starts are the standard contract forms supplied by the provider. It is worth noting, however, that growing number of cloud contracts nowadays appear to be subject to negotiation between customers and providers, and in parallel, during these negotiations, a larger number of T&Cs are being amended in their scope and in their nature, one of the reasons arguably being the customer's increased knowledge level.

Standard Terms/Non negotiated terms:
Most cloud services offer commoditised, non-negotiable, ‘click-through’ contracts to customers, especially when they are offering cloud services to consumers and SMEs. The terms of service in these contracts tend to be complex and obscure for the layman, and therefore it is often difficult for customers to understand what terms they are agreeing to. Many of the provisions in such contracts – especially the ones provided by common law, extra-European based providers – tend to favour providers and be disadvantageous to customers in a way which renders them possibly unenforceable or even illegal *tout court*.

Terms of Service (ToS):
This document contains terms relating to how the service is to be used and sets out terms relating to the relationship between the user and provider. Within this there may also be an Acceptable Use Policy (AUP).

B. Report on COAT experiment

Background Information

The legal partners involved in this Work Package (QMUL,TiU) ran an experiment with COAT in January 2015. The demo -recorded and produced by HP team- was presented to five (5) potential users of the tool acting in their capacity as end users (laymen) or businesses (SMEs). There were several viewings as interviewees needed to take time to respond, go back to previous questions or request for explanation. The experiment aimed both at giving insights for the work in parallel on the landing page of the tool/dummies guide as well as at improving the current demo (e.g. reordering questions).

The report below is composed of two sections: Section (I) focuses on how potential COAT users/SMEs reacted to COAT demo, while Section (II) captures reactions coming from potential COAT users/consumers. The first part of each section summarizes the main points of the interviews taken; remarks made concerning each question separately are addressed under the second part. The outcomes of the report were taken into account to improve shortcomings of COAT. Note that the discussion that follows covers feedback collected on prior version of COAT demo overall rather than on points raised linking to specific questions.

Section (I): COAT users-SMEs

The SMEs interviewed do businesses across different sectors, namely, seafood import, healthcare and e-commerce. Two of the SMEs (e-commerce/seafood import) were familiar with cloud offered services; they have been using them (e.g. services offered by Microsoft) for cloud storage and software updates. The same SMEs (e-commerce/seafood import) focused on the usability of the tool and on technical aspects of the questions, while the SME doing business in health sector often questioned the reasoning behind the chosen questions (e.g. "Why location matters?"). Note that the interviewees representing the SMEs are highly educated, aging from 29-59 years old, yet not all exceptionally technologically savvy.

General remarks

- They interviewees saw answering the questions in the tool more like an obligation they had to meet in order to get advice rather than like a filter that would limit the number of relevant offerings and –ultimately- help them make an appropriate choice tailor-made to the needs of their businesses. One SME clearly said: *"[The demo] misses the point a bit because it doesn't ask you want you need from cloud – so you could end up choosing the wrong thing or just not knowing the answer in the list. And the services are not comparable at all in the results list when it comes to storage because you don't know what volume you are buying."*
- It was not obvious how the tool actually compares offers; how does the tool come up with the proposed service providers?
- SMEs were primarily concerned about the price and the commercial features.
- The list of cloud services was considered too technical; Categories of cloud services shown are divided by technological features of cloud service SaaS, PaaS, IaaS. Most of the interviewees would chose based on functions or services they need in their business rather than categorised by cloud technology.
- All SMEs stated that there were more points that needed to be further explained aside from these already explained through pop ups. Also, one SME pointed out that the pop-ups were quite lengthy; the same SME pointed out that a pops could explain beforehand the consequences following from a certain answer. For, instance, if a certain answer is given, it was not entirely clear if the user of the tool would be exempted from certain questions that would appear later on screen.
- It was not obvious to them whether it was necessary to go through all questions, if they could go back and forth etc.; it seems, therefore, that the users treated the tool more like a questionnaire rather than as a tool enabling them filter their options.
- Language of major importance for all interviewees.
- Certification was not taken into account at all; SMEs were either indifferent (sea-food import, e-commerce) or ignorant.

- Different reactions when discussing location; SMEs would go either for strictly "Europe" or "Any"

Section (II): COAT users-individual end users

The end users interviewed were a student in Economics (age 21) and a graphic designer (age 28).

General remarks

- End-users pointed out the need for a front page actually saying what the tool is made for.
- End users considered that certain pages were crowded with information.
- Both users agreed that the tool was too long and that it would be useful, in this respect, to have a progress bar showing how far in the process they are; it appears that they used the tool as a questionnaire.
- Preferably as minimum clicks as possible. Certain questions, for instance, could be pre-selected (e.g. encryption).
- For one end–user there were certain questions entirely incomprehensible, namely, the ones addressing sub-contracting, providers' certification, demonstration of compliance, IPR, monitoring operations.
- Concerns by both end-users that everyone would go for the easiest choices ("any"/ "doesn't matter").
- One end user actually questioned whether there could a risk assessment when having to decide which provider to choose.
- End users queried for further information on how exactly the tool ended up proposing "matched offers"; on the basis of which criteria (e.g. reviews, popularity).
- Request for help in making the final choice out of the proposed set of choices. For example, one end-user proposed adding a list with "pros" and "cons" under each proposed offer.

Both SMEs and end users stressed that COAT does not ask them a basic question, which is "What do you need?". To a great extent points that have been taken for granted when developing the tool did call for additional explanation. For example, it was not clear to the interviewees if the question "Where are you?" meant to ask where exactly the user of the tool was physically located when going over the tool's questionnaire or if it implied home address or address of legal establishment. Moreover, certain interviewees requested for explanatory text in the front page of the tool, but also in the beginning of specific pages, as certain questions at that stage of development seemed problematic.

Index of figures

Index of tables