CLOUD ACCOUNTABILITY PROJECT

D:D-4.2 Report of survey of cloud standard contract terms and SLAs in 2015

Deliverable Number: D44.2

Work Package: WP D-4

Version: v0.4

Deliverable Lead Organisation: QMUL

Dissemination Level: PU

Contractual Date of Delivery (release): 30 June 2015 (M30)

Date of Delivery: 30 June 2015

Editor
Niamh Gleeson (QMUL)

Contributors
Niamh Gleeson (QMUL); Chris Reed (QMUL)

Reviewer(s)
Siani Pearson (HP), Dimitra Stefanatou (TiU)

SEVENTH FRAMEWORK PROGRAMME

Executive Summary

This deliverable presents the results of T:D-4.2 of Work Package 44 of the Cloud Accountability Project (A4Cloud). This paper is a public deliverable for the A4 Cloud project based on a survey of cloud contract terms finalized in June 2015. The research examined how cloud standard contract terms have evolved since an earlier survey of cloud contract terms in January 2013 conducted by Queen Mary University of London. The survey provides qualitative and some quantitative data about the evolution in cloud contract terms in that time period. The purpose of gathering this survey data is to examine whether these changes in standard cloud contract terms show an evolution towards more accountability by cloud providers in that two-year period.

This report first describes how the survey of cloud standard contracts has been conducted and the methodology for identifying the relevant cloud contracts for 2015; second it examines how cloud contract terms relate to the concept of accountability in the A4 Cloud project. It then examines the 20 most common contract terms to identify whether the cloud contracts in 2015 give evidence of improvements or amendments in service provider accountability since the survey in 2013. In addition to the survey of cloud contract standard terms, it also includes a survey and analysis of cloud SLAs and their relevance to accountability in 2015. This is because of initiatives from regulatory authorities and international standardization bodies to develop model or recommended SLAs for cloud. In addition, the cloud SLAs can be particularly relevant to accountability since they describe measurable targets by cloud providers in respect of their behaviour relevant to accountability attributes such as responsiveness and remediability. This report concludes with recommendations for best practices for accountability that serve as concrete outputs for A4 partners in their research on tools that use cloud contracts and SLAs.

Table of Contents

1 Introduction

This deliverable, D:D-4.2, forms part of the stream of work under T:D-4.2 of Work Package 44, entitled 'D-4: Contracts, SLAs, and Remediation' ('D4'), of the Cloud Accountability Project ('A4 Cloud').[1] The D-4 stream of work also involves development of software tools, for example, a tool called the Cloud Offering Advisory Tool or 'COAT' that helps customers chose a Cloud Service Provider that is appropriate for their data protection and security needs by performing a comparative analysis of Cloud Service providers. Based on the customer's answers' to a questionnaire, COAT draws up a shortlist of Cloud Offerings and a recommendation on which Cloud Service Providers' offer corresponds best to the customer's needs.

T:D-4.2 provides that Queen Mary University of London will undertake a survey of evolving contract terms and SLAs. This is to be an assessment of evolving cloud standard terms, based on a representative sample of providers offering services in Europe, to evaluate trends and innovations in cloud terms since the survey carried out as part of the A4 Cloud project in June 2013 as part of another work package, WP:B-5.4.[2] This survey is intended to provide qualitative data, and possibly also some quantitative data, about the developing treatment of accountability in the cloud market.

T:D-4.2 has two outputs, namely, an internal report MS:D-4.2 that was circulated at the end of February 2015 within the A4 Cloud project representing the preliminary findings and conceptual framework for the research and a formal deliverable D:D-4.2 due in June 2015 that is a public document.[3] This document represents the formal deliverable and as such gives the final analysis from the research findings ('June Report').[4]

1.1 Background and previous surveys on cloud standard contracts

The origin of the analysis in this report is based on surveys of standard cloud contracts that were carried out by Queen Mary University of London (QMUL), as part of its Cloud Legal

[1] A4 Cloud, Description of Works for Work Package 44 (as amended in August 2014).

[2] A4 Cloud internal briefing paper WP:B-5.4 Contractual and Regulatory considerations (WP25) June 2015,QMUL and TIU.

[3] Ibid.

[4] Ibid.

Project research, and published in 2010 and 2013.[5] The 2013 survey was also developed further for A4Cloud and forms the basis for the report WP:B-5.4 referenced above[6] and the 2013 survey has been referenced in other A4Cloud research concerning cloud contracts.[7] In brief, the earlier surveys are a reference point for research on cloud standard contracts, both within the A4 Cloud project and in the wider legal community.[8] Consequently, these surveys are the starting point in designing the current survey on cloud standard contracts in 2015.

In addition, using the same methodology as the earlier QMUL surveys ensures that valid comparisons can be made between the dataset collected in 2015 and the data from the 2013 survey. The methodology for gathering the data set for the survey in 2015, and the criteria used to identify and categorize cloud contracts used in this report for the survey conducted in 2015 are as close as possible to the methodology and criteria used in the 2010 and 2013 surveys by QMUL.[9] This is intended to ensure that any comparisons with the earlier contract terms are valid and based on comparable contract terms by the same cloud service provider. This methodology is described in further detail in the section 2 on survey methodology below.

1.2 Objectives

MS: D-4.2 investigates the evolution of cloud contracts over a two-year period. It draws on data collection methods, namely, documentary analysis of cloud contracts and on documents published by regulatory and legal authorities.

This research has two objectives: first, to collect qualitative and quantitative data on cloud standard contracts and their associated SLAs. The initial dataset concerns 30 cloud standard

---

[5] 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, sponsored by Microsoft. The authors are grateful to Microsoft for generous financial support that has made the Cloud Legal project possible.

[6] A4 Cloud internal briefing paper WP:B-5.4 Contractual and Regulatory considerations (WP25) June 2015,QMUL and TIU.

[7] A4 Cloud project document, internal discussion paper: 'MS:D4.1 Internal discussion document on drafting cloud computing terms' 17.10.2014, Lorenzo Dalla Corte (ed), TiU.

[8] The 2010 research paper has been downloaded over 6,800 times on SSRN, last checked on 26 February 2015.

[9] Bradshaw, Millard, and Walden, ibid. 2010 and 2013.

contracts and these are listed in Table 1 in the Annex to this paper. The analysis presented in this paper is based on this initial dataset collected in January 2015 and updated and checked in June 2015. This dataset is then used to make comparison with 30 cloud standard contracts surveyed in 2013. The contracts are comparing one-on-one the old contract (2013) and the new contract (2015) relating to the same service by the same cloud service provider. The research is intended to identify contract clauses that have changed and those that have stayed the same over this two-year period. The second aim of the research is to use the survey data to analyze the evolving treatment of accountability in the standard cloud contracts offered by cloud service providers. This involves developing a framework of analysis for assessing how cloud standard contract terms relate to accountability. It identifies which terms have changed most between 2013 and 2015 and assesses what this means for the evolution of accountability of the cloud service provider.

1.3 Structure

This Deliverable is divided into four sections (excluding this section). In section two, we set out the methodology for collecting the data set. We also describe the concept of accountability and how it can be related to cloud contract terms. In section three, we analyse the 2015 cloud standard contracts and in particular 20 cloud standard terms and assess how they have evolved since 2013 and what this means for accountability. In section four, we analyse cloud SLAs surveyed in 2015 and how they relate to accountability. In section five, we present our analysis of the findings of our research and our recommendations for best practice for accountability. Section six gives a short conclusion.

2 Survey Methodology

This section sets out how the 2015 survey was conducted, the scope of the survey, and the definition of cloud standard terms of service and the cloud standard terms used in the analysis.

2.1 Identifying survey data set in 2015 survey

The survey is restricted to a data set of standard contracts also called ‘terms of service’ from cloud providers. A cloud provider is any business organization that offers cloud services, whether IaaS, PaaS or SaaS. The criteria for choosing to include a contract in this survey is

based on the following factors:[10]

* ***Standard contracts, not negotiated*** –Standard contracts are those where the customer does not have the capacity to re-negotiate terms. The customer is therefore more likely to be a consumer or a SME rather than a large business; since larger businesses have more bargaining power to negotiate contracts with their cloud service provider. In addition, the contracts concern standard service offerings rather than more complex, negotiated or bespoke offerings.
* ***Publicly available, from website*** – The contracts surveyed are publicly available, downloadable from the relevant website of the service provider and a weblink is given for each contract
* ***Consistency with previous surveys*** – Service provider contracts aim to match the contracts examined in previous surveys in 2010 and 2013 in order to track the evolution of cloud terms. This is so that the contract terms surveyed concern the same provider and the same service offering. In some cases this has not been possible because either: the service provider has gone out of business; the service offering has changed significantly and the contracts are not about comparable services; or the standard contract was publicly available in earlier years but is no longer available from the provider's website. In most cases we have found a close alternative from the service provider's website, but where this has not been possible, they have been omitted from the study.
* ***Choice of English law or law of customer's region in the EU*** - Some cloud service provider websites offer customers a choice of contract depending on the region or country of the cloud customer. For the purposes of this analysis, we have chosen contract terms offered to a prospective customer under English law, or the law relating to the customer's region in Europe or the EMEA (Europe, Middle East, Africa) area.

The relevant date of the survey is 5 June 2015. The cloud contract terms were surveyed on 16 January 2015 and these contracts were re-examined in early June for any changes. Changes after 5 June 2015 do not feature in this report.

Based on the above criteria, Table 1, which is in the Appendix to this Deliverable, lists the cloud services that were covered by the survey in 2015 and a brief description of the type of service. Unless otherwise indicated, the cloud services are the same for previous surveys in 2010 and 2013. In total 30 contracts were reviewed for the 2015 survey from 29 different cloud

[10] This is the same as the criteria used in Bradshaw, Millard, Walden (2013), 40-44.

providers.

2.2 Definition of standard term contracts

Terms and conditions 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.[11] 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.

The documents can be defined follows: [12]

* **Terms of Service** (ToS). This document is often also called the terms and conditions and is the principle document that governs the relationship between the customer and the cloud service provider. It usually contains a range of typical legal clauses such as choice of law and limitation of liability clauses. This is the main focus of our survey, since the other documents are often incorporated into this document by reference.
* **Service Level Agreement** (SLA). This document specifies the level of service the provider aims to deliver together with the process for compensating customers if the actual service falls short of that. Typically, SLAs are associated only with paid-for services.
* **Acceptable Use Policy** (AUP). This document describes what the customer may and may not do with the service, usually with the sanction of immediate termination if the customer infringes this policy.
* **Privacy Policy**. This document describes how the cloud provider will protect personal information, and although called “Privacy Policy” most terms specifically relating to data protection.

In general, these documents are not discussed separately in the survey results. We analyze the terms of service together with the other documents, because together they constitute the entirety of the service contract. The exception is that we analyze our survey of SLAs separately since we believe that they are particularly pertinent to accountability.

[11] Consistent with the surveys conducted in 2010 and 2013, Bradshaw, Millard and Walden (2013) 43-44.
[12] See Bradshaw, Millard and Walden (2013), 43-44.

2.3 Analysis of cloud terms

The 2015 survey examines 20 main types of contract terms offered by cloud providers, consistent with the terms surveyed in 2010 and 2013.[13] Some examples of typical contract terms include: terms that set out the applicable law under which the contract is governed (applicable law clause); terms that set out whether the service provider has limited its liability under the contract (liability clause); and terms that concern the obligations on the service provider to retain or delete customer's data (data preservation clause).[14] Each provider's terms of service was analyzed against these 20 contract terms. The survey noted where there was significant variation from provider to provider.

These 20 clauses and a brief description of their role in a cloud contract are given in Table 2 to this document, which is given in the Appendix to this Deliverable.

The purpose of this survey in 2015 is different from earlier surveys. Its focus is specifically on the evolution of cloud contract terms in terms of accountability from the contracts surveyed in 2013 and the contracts surveyed in 2015. The analysis is not just about whether the contract terms have changed; but how far the changes demonstrate an evolution in accountability in the two years between both surveys. For this reason the framework for analysis needs to encompass the concept of accountability. The next section sets out how the concept of accountability relates to contract terms.

2.4 Accountability defined in A4 Cloud conceptual framework

Part of the challenge of addressing the issue of accountability in cloud computing was defining the scope of the concept of accountability. In order to do so, one work package of A4Cloud specifically addressed the Conceptual Framework for Accountability. The A4Cloud project has produced a model and framework for accountability published as a public Deliverable for the project.[15] The Conceptual Framework Deliverable for A4Cloud defines accountability within cloud ecosystems as follows:

> *Accountability for an organisation consists of accepting responsibility for data with which it is entrusted in a cloud environment, for its use of the data from the time it is*

[13] Bradshaw, Millard and Walden (2013), 44-64. These 20 terms were originally picked as the most common terms featured in cloud service provider contracts, at 39.
[14] Table 2 sets out the 20 contract terms with a brief description of each type of contract clause.
[15] A4Cloud D:C-2.1 Report detailing conceptual framework, 13.10.2014 (hereafter 'Conceptual Framework Deliverable').

> *collected until when the data is destroyed (including onward transfer to and from third parties). It involves the commitment to norms, explaining and demonstrating compliance to stakeholders and remedying any failure to act properly.*[16]

In addition, the Conceptual Framework Deliverable also defines a model of accountability, in which it identifies accountability attributes, and describes accountability practices and accountability mechanisms.[17] Most relevant to our research for this Deliverable is the description of the accountability attributes that defines the elements and properties of accountability at the conceptual level. These core attributes of accountability described below are used in our analysis of contract terms.

2.5 Core attributes of accountability

The Conceptual Framework Deliverable identified five key or core attributes of accountability related to a 'system', by which is meant (parts of) the accountable cloud ecosystem.[18] These are briefly summarized below:

Transparency: defined as 'the property of a system, organisation or individual of providing visibility of its governing norms, behaviour and compliance of behaviour to the norms. Being transparent is required not only with respect to the identified norms, behaviour and compliance within the cloud ecosystem, but also with respect to remediation. Transparency can be argued to be the most important attribute of accountability.

Responsiveness: the property of a system, organisation or individual to take into account input from external stakeholders and respond to queries of these stakeholders. Responsiveness in the context of cloud computing refers to the two-way communication relation between cloud providers and external stakeholders (such as individual cloud customers and regulators) needed within the cloud ecosystem to define part of the governing norms. Generally speaking, the audience for an organisation's account should somehow be involved with the process by which the account is produced, and not only with the product.[19]

Responsibility: the property of an organisation or individual in relation to an object, process

[16] Conceptual Framework Deliverable, 30.
[17] Ibid, 30.
[18] Ibid.
[19] Ibid.

or system of being assigned to take action to be in compliance with the norms. For each object, process or system within an accountable ecosystem a responsible entity (i.e. cloud actor that here would be the accountor) should be provided.

Remediability: the property of a system, organisation or individual to take corrective action and/or provide a remedy for any party harmed in case of failure to comply with its governing norms. The remediability attribute provides assurance that being responsible, etc. is not sufficient and further action is required in order to be accountable; although legal responsibility, namely liability, leads to remedies, accountability equally puts emphasis not only on whom to blame but how to repair the damage.

Verifiability: the extent to which it is possible to assess compliance with accountability norms. This is a property of the behaviour of a system, service or process that it can be checked against norms. It is considered to be a core attribute because accountability is explained in terms of defining and displaying relevant norms, behaviour and compliance to the norms.

2.6 Secondary attributes of accountability

The Conceptual Framework also identifies several secondary attributes of accountability.[20] They are secondary, since they are dependent on one of the key or core attributes of accountability and flow from them. For the purposes of research we will concentrate on primary accountability attributes. The only secondary attribute of accountability that we will give equal focus for the purposes of this research is liability. It is defined in the Conceptual Framework report as follows:

Liability: the state (of an organisation or individual) of being legally obligated or responsible in connection with failure to apply the norms. Liability is the legal obligation (either financially

[20] The secondary accountability attributes are as follows: *Attributability:* the possibility to trace a given action back to a specific entity. This is a property of behaviour or of a norm violation. *Observability*: the extent to which the behaviour of the system is externally viewable. There are other attributes of accountability, but they may be defined to capture the important aspect of deployment of 'appropriate and effective measures' that meet technical, legal and ethical compliance requirements, and act as this type of indicator. These are: *Appropriateness*: the extent to which the technical and organisational measures used have the capability of contributing to accountability; and *Effectiveness*: the extent to which the technical and organisational measures used actually contribute to accountability. We will not take them into account in our analysis because, in the case of attributability, observability and effectiveness, these attributes relate to the evidence that the core accountability attributes have been adhered to by an organization. Therefore, they cannot be mapped in abstract to contract terms. In the case of appropriateness, this is context dependent and consequently cannot be mapped to contract terms.

or with some other penalty) in connection with failure to apply the norms. It is closely related to legal responsibility (although being held liable does not necessarily mean that the same entity is actually responsible), and because it is not referred to directly in our definition, and so could be considered to be a secondary attribute.[21]

For the purposes of analyzing contract terms, liability can be considered as an important attribute of accountability in relation to a legal relationship and for legal analysis. We will therefore use the term 'responsibility and liability' together when referring to these attributes of accountability in our analysis.

2.7 Relationship between contract terms and accountability[22]

Each of the 20 contract terms analyzed as part of the 2015 survey is assessed against the core accountability attributes. This gives us a framework of reference for assessing an increase or decrease in accountability in the contract terms between 2013 and 2015. It should be noted that some clauses could be relevant to several accountability attributes, while others are only slightly relevant or peripheral to accountability.

3 Standard cloud contracts and analysis of the 20 key terms

This section examines in detail the contract terms from the cloud standard contracts surveyed in 2015 as part of the A4Cloud project under T:D4.2. Its focus is specifically on the evolution of cloud contract terms in terms of accountability from the contracts surveyed in 2013 and the contracts surveyed in 2015. The 20 typical contract terms are listed in Table 2 in the Appendix.

These 20 terms were divided into three broad categories for the purpose of analysis in 2013.[23] These three categories are: first, contractual form and applicable law, which includes all clauses about applicable law, jurisdiction, arbitration and payment; second, data handling which includes clauses about data retention, deletion, transmission and storage; and a third category on liabilities and responsibilities, which includes clauses on warranties, direct and indirect liability.

[21] Conceptual Framework Deliverable,31.
[22] The relationship between contractual terms and accountability is also discussed, particularly in relation to transparency, in the context of drafting cloud terms as part of the A4 Cloud project in the document: 'MS:D4.1 Internal discussion document on drafting cloud computing terms' 17.10.2014, Lorenzo Dalla Corte (ed), pp 16-24 in particular.
[23] Bradshaw, Millard and Walden used these categories for analysing the 2013 survey. 44

For the purpose of our analysis concerning contract terms and accountability, the first and third categories are closely related, in that their provisions are all primarily relevant to dealing with any disputes or failures that arise during the course of service provision. These categories could be classified as related to "dispute handling" dealing with liability and the mechanism for resolving potential legal disputes concerning liability (for example, applicable law, courts etc). Cloud service providers are unlikely to offer any service levels in relation to these matters because they can only be resolved through negotiation or, ultimately, legal action. By contrast, the data handling provisions are promises about what the cloud service provider will do in relation to the customer's data, ie promises about performance of the services. This is an area where service levels are more likely to be offered, and therefore are relevant to Service Level Agreements (SLAs) though as we shall see in part 4 the current approach to service levels is limited to a very narrow element of such performance.

3.1 Applicable law

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 of business. Out of the 31 terms of service analyzed in 2010 and 2013, just over half of the providers specified the law of a particular US state.[24] The 30 terms of service surveyed in 2015 repeated this trend.

In the 2015 survey, most of the US cloud providers surveyed gave the governing law as being the law of a US state, usually California,[25] although there were a few providers that chose other

[24] See Bradshaw, Millard and Walden, at 46, with a table setting out the breakdown of choice of law per jurisdiction for 2010 and 2013.
[25] Clause 19, ADrive 'Terms of Service' (5 January 2015) and available at http://www.adrive.com/terms and last accessed on 5 June 2015; Clause 'Controlling Law' Dropbox 'Dropbox Terms of Service' (1 May 2015) available at https://www.dropbox.com/terms and last accessed on 3 June 2015; Facebook 'Statement of Rights and Responsibilities ' (30 January 2015) available at https://www.facebook.com/legal/terms and last accessed 3 June 2015; Clause 8.8 'Choice of Law and Jurisdiction' GoGrid'Terms of Service' (22 November 2013) available at http://www.gogrid.com/legal/terms-service and last accessed on 3 June 2015; Clause 'About these terms' in Google Google 'Google Apps for Business (Online) Agreement' (28 March 2012) available at https://www.google.com/intx/en_in/work/apps/terms/2013/1/premier_terms.html and last accessed on 4 June 2015; Clause 21 'Governing Law' Joyent 'Terms of Service' (3 April 2014) available at https://www.joyent.com/about/policies/terms-of-service and last accessed on 4 June 2015; Clause 16 in Norton 'Norton Online Backup Terms of Service Agreement' (undated) available at https://nobu.backup.com/terms_of_service and last accessed on 5 June 2015.

states: the laws of Delaware,[26] Washington,[27] New Jersey[28] and New York state.[29] Some other non-EU providers specified the governing law of their home jurisdiction: Canada[30] and New Zealand.[31] The majority of the rest of the terms of service gave the governing law as the laws of England and Wales for contracts in English.[32] This reflects the fact that in conducting the survey, where there was a choice of terms of service from the cloud provider based on geographical location, we chose those appropriate to a customer based or receiving service in the UK.

Evolution in terms of accountability

The results however hide some of the subtler changes since 2013 that indicate an evolution in terms of awareness by cloud providers that EU citizens or consumers may need to be allowed to use the applicable law in their country of residence. Notably, several cloud providers specify the laws of a US state, but make an exception for citizens of EEA. For example, iCloud Terms of Service specifies the laws of the State of California as applicable law, but then provides an exception for EU citizens and citizens of Switzerland, Norway and Iceland 'the governing law

[26] Clause 23 'Governing Law' in SavvisDirect 'Terms and Conditions' (1 June 2015) available at https://apps.centurylink.com/terms-conditions and last accessed on 5 June 2015.
[27] Clause 13.11 'Governing Law' in Amazon Web Service 'AWS Service Terms' (23 April 2015) and available at http://aws.amazon.com/service-terms/ and last accessed on 5 June 2015; and Mozy by EMC 'Mozy Terms of Service' (11 June 2014) available at https://mozy.com/about/legal/terms and last accessed on 3 June 2015.
[28] Linode 'Terms of Service' (undated) available at https://www.linode.com/tos and last accessed on 5 June 2015
[29] IBM 'Cloud Services Agreement' (undated) available at http://www-05.ibm.com/support/operations/files/pdf/csa_us.pdf and last accessed on 4 June 2015; and Softlayer 'Master Service Agreement' (March 2014) available at http://www.softlayer.com/legal and last accessed on 5 June 2014.
[30] 500px specified the law of Ontario.500px 'Terms' (9 August 2012) available at https://500px.com/terms and last accessed on 5 June 2015.
[31] Mega gave New Zealand law. Mega 'Mega Limited Terms of Service' (undated) available at https://mega.co.nz/ios_terms.html and last accessed on 5 June 2015.
[32] Elastichosts 'Elastichosts Terms of Service, SLA & AUP' (undated) available at http://www.elastichosts.com/cloud-servers/terms-of-service/ and last accessed on 3 June 2015; Flexiant 'Terms of Use' (undated) available at https://www.flexiant.com/terms-of-use/ and 'Flexiant Cloud Orchestrator End User licence agreement' (undated) available at https://www.flexiant.com/support/eula/ and last accessed on 3 June 2015; PayPal 'User Agreement for PayPal Service' (15 April 2015) available at https://www.paypal.com/uk/webapps/mpp/ua/useragreement-full?locale.x=en_GB and last accessed on 5 June 2015; Rackspace 'Cloud Terms of Service' (13 November 2014) available at http://www.rackspace.com/information/legal/cloud/tos and last accessed on 5 June 2015; Salesforce 'Cloud Master Subscription Agreement' (1 September 2014) available at http://www.salesforce.com/company/legal/agreements.jsp and last accessed on 5 June 2015; Canonical ' Ubuntu One Terms of Services' (January 2014) available at https://login.ubuntu.com/terms/ and last accessed on 5 June 2015.

and forum shall be the laws and courts of your usual place of residence'.[33] Several other US providers have a section in their contract with "country specific terms" that gives different governing law depending on the region. For example, Rackspace provides that services from UK are governed by the laws of England and Wales. Microsoft's terms of service give a wide range of jurisdictions depending on the region, with Luxemburg being the law applying to most EU jurisdictions.

Another development is that cloud providers appear to be aware that consumer laws may make their choice of law or applicable law provisions in their contracts redundant. One provider provides explicitly that the applicable law provisions are without prejudice to any consumer law or rights "Nothing in this clauses is intended to prevent any consumer that is a Customer from relying on the consumer law applicable in the jurisdiction in which the Customer resides".[34]

Therefore, there are increasing choice of law provisions and increased awareness that consumer law may apply irrespective of the governing law chosen by the cloud provider. This is a promising development from the point of view of accountability.

Significance for accountability

The choice of law clause it relevant to three attributes of accountability, namely, remediability, transparency and liability. 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. It affects the remedy available for any party harmed in case of failure to comply with the cloud contract. 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 could bring a legal action. This is particularly the case where the choice of law specifies another continent and particularly another legal system and language. The most relevant clauses in the contract concerning remediability are the clauses concerning applicable law, jurisdiction and dispute resolution, since these are all highly relevant in how easy or difficult it is to bring a legal claim against the cloud service provider. Remediability encompasses undertakings or mechanisms that are designed to fix or repair the breach. Understanding the applicable legal obligations is part of this process. The expense of hiring legal counsel who are expert in the foreign law system

[33] Clause X.B Governing Law, in Apple 'iCloud Terms and Conditions' (20 October 2014) and available at http://www.apple.com/legal/internet-services/icloud/en/terms.html and last accessed on 5 June 2015.
[34] Box 'Box Terms of Service' (4 August 2014) available at https://www.box.com/legal/termsofservice/GB/ and last accessed on 5 June 2015.

may make companies think twice before they insist on their legal rights in the contract or consider what are their remedies.

Also, applicable law affects interpretation of contracts. Although many businesses are confident that they understand in general terms how their local contract law applies to their dealings, they may not be so confident that they understand contracts that are to be interpreted under foreign law. 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.

Choice of law terms may be more significant for corporate and particularly for SME customers since individual consumers may be helped by consumer protection law that protect them from having a foreign legal system imposed on them.

3.2 Jurisdiction

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 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.

Significance for accountability

Jurisdiction for a dispute is relevant to accountability since it relates to remediabilty 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 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.

3.3 Arbitration

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. Bradshaw, Miller and Walden suggest that cloud providers that tried to impose arbitration as a dispute resolution mechanisms only did so in relation to certain jurisdictions only, and that generally these terms reflected a lack of confidence in the judicial system.[35]

Nevertheless, the surveys in 2010 and 2013 indicate that over a quarter of cloud service provider included some type of clauses seeking to impose arbitration to resolve disputes.

This was confirmed in the 2015 survey where a quarter of providers included arbitration clauses for dispute resolution.[36] Most of the arbitration clauses make reference to a forum for arbitration or recognized rules of arbitration, usually the American Arbitration Association rules.[37] In addition, many arbitration clauses prohibit consolidating claims, so the use of the arbitration clauses may also be a mechanism to prevent class actions.

Significance for 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. Compulsory arbitration clauses against consumers are usually not enforceable. 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.

[35] Bradshaw, Millard and Walden (2013), 49, noted that compulsory arbitration clauses by certain cloud providers only related to specific jurisdictions, for example, the Republic of China and states within the former Soviet Union.

[36] The providers that had arbitration clauses were Savvis direct, Adrive, Dropbox – which had mandatory arbitration but for US citizens only, Zoho and Mega.

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

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.

3.4 Acceptable use clauses

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 tend to prohibit the following range of activities: spam, fraud, gambling, hacking, hosting content that is obscene, defamatory or illegal or discriminatory.[38] The survey in 2015 showed no change from the survey in 2013.

Significance for 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, it shows transparency by the cloud provider. 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.

3.5 Variation of contract terms

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

[38] 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.

as their consent or acceptance of the new terms. A very small number state - just two providers - that any changes to their terms of service could only be made with the consent of both parties.[39] Some providers stated that they would email customers about any contract changes, but that continued use of the service constituted consent to the contract changes. The provisions on change of contract terms have not noticeably changed between the surveys in 2013 and the survey in 2015.

Significance for accountability

The most relevant accountability attribute is transparency since the contract changes need to be transparent for the customer to understand what has changed in its contract. It also relates to the secondary attributes of appropriateness and effectiveness. This practice of sending a unilateral notice of changes to the cloud customer, by posting of contract changes on a website, is neither transparent and, for material contract changes it is not appropriate 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 is not appropriate and does not demonstrate accountability. The majority of customers would not check and would be entirely unaware if and when their cloud terms of service had changed. Therefore, a balance needs to be struck between giving information to customers in an accountable way about contract changes and having an appropriate and proportional response by cloud service providers. Consumers are more protected than SMEs customers since unilateral changes to contracts without notice to the consumer could be regarded as unfair under the relevant EU Directive 93/13/EEC on unfair terms in consumer contracts, as transposed into national law.

3.6 Data integrity

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

[39] Bradshaw et al, 51.

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.

Significance for 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 may have a regulatory responsibility as a data controller that it cannot just exclude by a contractual clause.[40] 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.

3.7 Data retention and deletion

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 a customer who wants to transfer or recover their data in a managed manner. The surveys of cloud contracts found that providers deal with data retention or deletion of customer information following the end of the contractual relationship in the following three ways:[41] first, providers retain customer data for a set period after the end of the contract, often 30 days; second, providers delete customer data immediately at the end of the customer relationship; third, 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. There were no noticeable changes to these terms between the 2013 survey results and the 2015 survey.

Significance for accountability

[40] Under the Data Protection Directive.
[41] 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.

The accountability attributes concerns first, transparency, by stating how long the data will be preserved at the end of the contractual relationship with the customer and, second, responsiveness to the customers need to port or to ensure deletion of certain data. 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. Many customers require data reversibility or data portability and the ideal is that the cloud provider guarantees the easy reversibility or portability of the data in a structured and widely used format, at the customer's request and at any time.[42] In addition, they need a grace period before their data is deleted after the contract ends.

3.8 Data disclosure to LEAs

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 in 2013 and again in 2015.[43] 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 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.[44]

Significance for accountability

[42] CNIL recommendations
[43] 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.
[44] 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-lawsuit

This clause concerns the accountability attributes of transparency and responsiveness. Disclosure for law enforcement in circumstances where there is a valid court order is entirely reasonable. 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 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.

3.9 Data location and transfer

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.[45] However, most cloud providers surveyed in 2013 did not state explicitly in their terms of service where they will store data. The survey in 2015 shows that more cloud provider specify where their data will be transferred or stored. This is sometimes part of the sign up process: where users may be able to chose a region where their data is stored. In addition, some providers indicate compliance with the US Safe Harbor obligations, sometimes as part of the Privacy Policy.

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.

Significance for accountability

Since this is such a key issue for customers, it is surprising that 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.

[45] Directive 95/46/EC (OJ L281/31, 23.11.1995).

3.10 Monitoring by provider

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 concerns 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 surveyed in 2015, but not all, contain a clause where the provider acknowledges that it will monitor customer data and states the purpose of such monitoring. This does show any evolution since the survey in 2013.

Significance for 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 purpose of the monitoring is 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. Instead, most cloud providers are silent on this point. Nevertheless, the monitoring appears to be generally to detect a breach of the AUP, which a customer in breach is unlikely to acknowledge, so it seems proportionate that the CSP can monitor this, particularly if it risks legal liability.

3.11 Rights over service and content

This clause appears in cloud contracts concerning intellectual property (IP) rights over content and data uploaded to the cloud by customers. Most cloud contracts surveyed in 2015 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 servicer remains the property of the content owner. This means that IP in customer data remains with the customer. This has not changed from the survey in 2013.

Significance for accountability

No particular impact from accountability.

3.12 Other proprietary rights and duties

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

Significance for accountability

Since this does not feature in most contracts, there are no consequences from the point of view of accountability.

3.13 Warranty

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 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. This position has not changed from the survey in 2013.

Significance for 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.

3.14 Direct liability

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 direct liability, although the cloud terms of service by US cloud providers contain much more extensive liability exclusions than other cloud providers. Several specify exactly what is included in direct breach for the avoidance of doubt. In most cases, particularly in contracts with US providers, these clauses are in capital letters so that the

disclaimers on liability are conspicuous and not hidden in the contract.[46] The liability exclusion clauses surveyed in 2015 do not differ from the same clauses surveyed in 2013.

Significance for 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.

3.15 Indirect liability

Most contracts make a distinction between two different types of liability, direct and indirect liability. Direct losses or injury that are foreseeable consequences of the breach of contract fall within direct liability. In English law, indirect losses concern losses that are more remotely connected with the breach of contract. The party at fault will only be liable if there are special circumstances known to the party at fault 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 mean that the customer will automatically lose a lucrative government contract; or that a service failure will cause delays in the customer's product delivery system that means it incurs penalties for late delivery to its customers. In these circumstances, such losses (loss of a lucrative contract or 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. In English law they are also called consequential losses and these losses can include physical damage, loss of profits, economic losses and damage to goodwill and reputation. In some common law systems, such as Australia, indirect losses refer to economic losses such as loss of profits, as opposed to physical damage or loss that are considered direct losses. Most contracts try to exclude indirect losses because they are unpredictable. They represent unquantifiable 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

[46] This reflects requirements in the US Uniform Commercial Code and many warranties and disclaimers in cloud contracts are in capital letters.

these clauses especially from US cloud service provider appeared in capital letters. This meant that the cloud service providers' exclusion of indirect liability did not change from the 2013 survey.

Significance for 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 consumer protection legislation. Therefore, there are no particular recommendations on best practice as regards clauses limiting indirect liability.

3.16 Limit of liability (liability cap)

These are clauses that impose a limit or cap on the amount of damages that should be paid in the event that the cloud service provider 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!). There was no noticeable difference or evolution in this clause between the survey in 2013 and the survey in 2015.

Significance for 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, this type of liability cap is unlikely to be enforceable in English law against a consumer.

3.17 Indemnification

An indemnity clause means that the customer gives an obligation to provide compensation for future loss or damage. Consistent with the previous survey in 2013, 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.

Significance for 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 best practice to add.

3.18 Service availability

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 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. This is consistent with the survey results for this clause in 2013.

Significance for accountability

This clause relates more to quality of the service than to accountability. This is another example of a clause that generally excludes or limits cloud provider responsibility for the service. The only advantage of such a clause from an accountability point of view is the fact that it is transparent. Business customers, especially, bigger business customers, may have the possibility of arguing for greater service performance availability in the context of a service level agreement.

3.19 Service credits

Service credits are a way of compensating customers for failure to deliver the service to agreed levels. This is normally a feature for commercial services that offer a discount on the next invoice rather than monetary compensation. 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. The survey in 2015 showed that these mainly featured in the SLAs and, as such, are analysed with the standard cloud SLAs in the next section of this document. There does not appear to be any significant difference or evolution in this clause in the 2015 contracts surveyed from the 2013 survey.

Significance for 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 engage in litigation, hire a lawyer or threaten the service provider with legal action.

3.20 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. The difference is that for free services there is no periodic payment structure and thus no fixed contract term. The terms of payment clauses surveyed in 2015 do not differ in any respects from those surveyed in earlier years.

Significance for accountability

This clause does not have any particular relevance from an accountability point of view.

3.21 Conclusion on evolution of the 20 key contract terms in cloud standard contracts

[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.

The analysis on cloud standard terms indicates that most contract terms have not evolved significantly between the survey carried out in 2013 and the 2015. Therefore, there has not been a huge revolution in cloud standard terms leading towards more accountability. Nevertheless, from our analysis, two factors show a promising trend towards more accountability. First, more cloud providers in 2015 are more likely to offer regional variations on standard contracts to their customers. This means that the applicable law and relevant jurisdiction for disputes are likely to be in the country, or perhaps the region, where the customer is resident or has his place of business. Customers that have a contract under an applicable law with which they are familiar and that can bring disputes to a court that is in their country or region are in a much stronger position as regards relying on their legal rights in the contract. Therefore, the regionalisation of cloud contracts (as opposed to having world-wide standard contracts) is a positive step since it makes the cloud provider more accountable to the customer. Second, many cloud providers now explicitly acknowledge whether or not they will transfer or store data outside certain regions. The have more extensive privacy policies that describe how data will be treated and transferred geographically. This is important for customers to understand compliance with data protection rights and privileges.

However, there are a wide variety of clauses that show no change between the surveys in 2013 and 2015. These are the liability and warranty clauses that attempt to strictly limit the cloud provider's liability. Cloud service providers are unlikely to change these clauses by themselves. The only realistic likelihood for change for these clauses is through enforcement activity from national regulatory or consumer authorities, such as the Competition and Markets Authority (CMA) in the UK.

The terms where there are promising possibilities of development towards accountability in the future are the 'data handling' clauses, those clauses dealing with data integrity, data preservation, data retention, data location and transfer, and data disclosure. Recent initiatives to develop model cloud service level agreements concern obligations that relate particularly to data handling. Therefore, the developments with cloud service level agreements may be the most promising factor leading towards the evolution of accountability for cloud standard contracts. For this reason, cloud service level agreements are dealt with separately in the section that follows.

4 Service Level Agreements

This section deals with the analysis of Service Level Agreements or SLAs that are part of the contractual agreement between the cloud service provider and the customer. They fall within

the terms of service but, nevertheless, they are often a separate document and their content varies significantly from standard contract terms. SLAs are often used to specify actions that will be taken by the cloud service provider, usually relating to performance and availability.

4.1 Separate analysis of SLAs

In 2013, the SLA was included with all documents relevant to cloud contract terms that were dealt with under the umbrella term ‘terms of service’. In 2015, for the first time, the SLAs are surveyed and analysed separately from the terms of service.

This difference between the earlier survey in 2013 and this survey is for two reasons. First, there has been significant number of initiatives from regulatory authorities and international standardization bodies to develop model or recommended SLAs for cloud. These initiatives and their relevance to accountability are described below. Second, the SLA is often used by cloud service providers to give commitments to measurable service targets, for example, by committing to response times for service failure. Third, SLAs could be used to explain the meaning of contract terms by setting out what the provider will actually do. For example, in the case of data integrity, the customer may be legally responsible, but the CSP could specify what it would do in the event of service failure, what business continuity plan it will put in place to assist or provide a limited remedy in the case of failure. Therefore, the cloud SLAs could be particularly relevant to accountability since they describe measurable targets by cloud providers in respect of their behaviour relevant to accountability attributes such as responsiveness and remediability.

For these reasons, this 2015 survey analyses the SLAs separately from the general terms of service for the first time. This presented some methodology issues as regards the survey. First, this research cannot show the evolution of accountability in cloud contracts and SLAs because the initial research survey undertaken in 2013 did not isolate SLAs from the terms of service, we do not have a comparative data set from 2013 to describe how SLAs have evolved from 2013 to 2015. However, it is still possible to analyse the SLAs in 2015 from the point of view of accountability, and this work will provide a starting point and baseline for future surveys or assessments of accountability. The second methodology issue with collecting the SLA dataset concerned the more restricted number of providers offering SLAs. SLAs are a feature of cloud service providers’ offerings to professional users only; consumers typically are not offered an SLA. Therefore only a sub group of the Cloud Service Providers surveyed for their terms of service offered an SLA associated with the service.

By examining a small but representative sample of SLAs in 2015 we can identify how aspects of SLAs are relevant to accountability, for example, in terms of quantifiable performance measures, evidence and remedies. This can be used for assessing how SLAs relate to accountability and for recommendations on how SLAs could contribute to accountability.

4.2 Regulatory initiatives on cloud SLAs

Model SLAs and standardised service descriptions that include consistent and comparable service terminology have been a feature of calls for standards in cloud.[48] Without standardised descriptions of cloud services, buyers may find it difficult to understand what they are buying and cannot easily compare services or determine the relative value of offerings. On the one hand, such informational standards can be viewed as a demand-side measure designed to facilitate competition in the cloud market.[49] They are also relevant to accountability, in that they increase transparency and build trust by cloud customers.[50] There are several entities at regional and international level involved in trying to develop standardised SLAs and model contracts for cloud. These initiatives and recommendations are taken into account when assessing the SLAs surveyed in 2015.

4.3 EU initiatives on standardized cloud SLAs and model contract terms

The European Commission in its Cloud Strategy Communication identified the development of model terms and service level agreements as being a key action points in its consultation on cloud strategy.[51] The European Telecommunications Standards Institute (ETSI) in its report

[48] In Commission Communication, at 11, but see also the US Government Cloud Computing Technology Roadmap Requirements Volume I, November 2011, which identifies 'High quality service-level agreements' at 17. Also private standards development organisations like the Cloud Standards Customer Council 'Practical Guide to Cloud Service Level Agreements', April 10 2012. Accessed at: http://www.cloudstandardscustomercouncil.org/2012_Practical_Guide_to_Cloud_SLAs.pdf

[49] For a distinction between different types of cloud standards, see Gleeson and Walden 'Cloud Standardisation: It's a Jungle Out there' ITLJ, 2014.

[50] Although we do not specifically address the secondary attributes of accountability, this appears to relate to the attribute of 'observability' since by covering technical parameters not addressed in the contract, SLAs may make technical systems more observable.

[51] In Commission Communication, at 11, but see also the US Government Cloud Computing Technology Roadmap Requirements Volume I, November 2011, which identifies 'High quality service-level agreements' at 17. Also private standards development organisations like the Cloud Standards Customer Council 'Practical Guide to Cloud Service Level Agreements', April 10 2012. Accessed at: http://www.cloudstandardscustomercouncil.org/2012_Practical_Guide_to_Cloud_SLAs.pdf

on standards in cloud, following from the European Commission strategy,[52] identified the characteristics of the ideal standardised service level agreement for cloud. Service level targets for cloud need to be *well-defined*, so that cloud suppliers should not be able to interpret measures differently; *determinate*, so that multiple measurements of identical systems in identical states must give the same result; *correlated* to business value or to real-world performance of typical consumer tasks; and *comparable*, so that metrics reflect the same quantity across different measurement targets.[53] The value of comparable metrics has already been recognised in the telecommunications sector, as well as other utility markets, and an obligation to supply appropriate data can be mandated for providers.[54]

Subsequently, there have been two European Commission policy initiatives that are particularly relevant to standardised or model cloud contracts and SLAs:

4.3.1 Cloud Select Industry Group on cloud computing

The Cloud Select Industry Group (C-SIG)[55] is a working group set up by the European Commission to deal with various cloud computing issues. There are three sub-groups: one working group focuses on SLAs for cloud computing, one focuses on data protection in cloud computing and one focuses on certification for cloud computing. These work with industry to agree on norms for different aspects of cloud service.

The Cloud Select Industry Group on developing cloud computing Service Level Agreements deals with contracts between cloud providers and enterprise cloud users.[56] In June 2014, this group published its guidelines aimed at business cloud customers, the Cloud Service Level

[52] ETSI CSC Report.
[53] ETSI CSC Final Report, 7.
[54] For telecommunication providers, see Directive 2002/22/EC on 'universal services and users' rights relating to electronic communication networks and services' (as amended), at article 22(2). For other utilities, see the Enterprise and Regulatory Reform Act 2013, ss. 89-91.
[55] There is no formal Commission decision setting up the Cloud Select Industry group and its sub-groups, although it is linked to the Directorate General for the Information Society ('DG Connect') and meetings and minutes of the working groups are set out on the DG Connect website.
[56] https://ec.europa.eu/digital-agenda/en/cloud-select-industry-group-service-level-agreements on 10 January 2014.This group interfaces with the ETSI group mapping standards for SLAs see Report of the first meeting of the Cloud Select Industry Group – Service level agreement expert subgroup held on 21st of February 2013, p.2. Accessed at: https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/22022013%20Report_1%20SLA%20group.pdf. The website of ETSI Taskgroup on SLAs is available here: http://csc.etsi.org/website/home.aspx

Agreements Standardisation Guidelines.[57] The guidelines set out principles for the development of SLAs standards for Cloud Computing. The guidelines also set out typical Service Level Objectives or 'SLOs' that cloud providers could give in the SLA. SLOs are objectives set out by the cloud service provider for the performance of the cloud service and the performance of related aspects of the interface between the cloud service customer and the cloud provider.[58] The SLOs in the guidelines are divided into four categories: Performance SLOs, Security SLOs, Data Management SLOs and Personal Data Protection SLOs.

Performance Service Level Objectives[59] These relate to the performance of the cloud service and the interfaces between the cloud service customer and provider. These cover: availability (the property of being accessible and usable upon demand, also called 'uptime'),[60] response time (refers to the interval between a cloud service customer initiated event and a cloud service provider initiated event in response to the stimulus), [61] support (an interface made available by the cloud service provider to handle issues and queries raised by the cloud service customer. Relevant SLOs relate to support responsiveness and resolution time (p18). Reversibility and termination process refers to the series of steps that enable a customer to retrieve their cloud service customer data within a stated period of time before the cloud service provider deletes the cloud service customer data. The relevant SLAs relate to the data retrieval period and the data retention period.

Security Service Level Objectives cover SLOs relating to service reliability, authentication and authorisation, cryptography, security incident management and reporting, logging and monitoring, auditing and security verification and vulnerability management.[62]

Data Management SLOs include data classification, cloud service customer data mirroring, backup and restore, data lifecycle and data portability.[63]

[57] https://ec.europa.eu/digital-agenda/en/news/cloud-service-level-agreement-standardisation-guidelines
[58] Cloud Service Level Agreement Standardisation Guidelines, published by the Cloud Select Industry Group (C-SIG) on SLA I, set up by DG Connect to work on SLAs. Guidelines published on 24 June 2014, Brussels and available at https://ec.europa.eu/digital-agenda/en/news/cloud-service-level-agreement-standardisation-guidelines and last accessed on 8 June 2015.
[59] Guidelines, 15-19.
[60] p15
[61] p16
[62] pp 20-26.
[63] pp 44-50

Data protection SLOs include codes of conduct, standards and certification mechanisms, purpose specification data minimization, use retention and disclosure limitation, openness transparency and notice, accountability, geographical location of cloud service customer data, intervenability.

Relevance to accountability attributes The SLOs described in these guidelines are directly relevant to accountability attributes such as transparency, responsiveness and verifiability, for example SLOs relating to logging and monitoring, auditing and security verification and support response times. SLOs relating to logging and monitoring cover matters such as the records and data related to the operation and use of a cloud service. These are usually the responsibility of the cloud service provider and are intended to give cloud service customers the ability to analyse incidents such as security breaches and service failures as well as monitoring the customer's day-to-day use of the service. For this reason, those SLOs would map with the accountability attribute of verifiability and also transparency. Similarly, SLOs relating to support and support responsiveness, which specifies the maximum time the cloud service provider will take to acknowledge a cloud service customer inquiry or request and target resolution time for customer requests,[64] address the attribute of responsiveness. Many SLOs are directly relevant to remediability, for example, provisions regarding security incident management and reporting, can describe how these incidents are reported to the customer, how they are assessed and acknowledged and how they soon they are resolved after discovery.[65] In addition, in relation to data protection, there is a specific SLO for accountability, relating to data breach policy by the cloud service provider.[66] For this reason, SLAs have a special significance for demonstrating accountability by cloud service providers.

In the preamble to the guidelines, the authors acknowledge that the initiative will have maximum impact only if implemented at the international level rather than purely at the regional level and, to this end, the guidelines form the basis for the submission by the C-SIG SLA subgroup as the European Commission expert group to the ISO/IEC JTC 1 Working Group on Cloud Computing which is currently working on an international standard for Cloud SLAs. [67]

[64] Ibid, 16.
[65] Ibid, 23.
[66] Ibid, 35.
[67] ISO/IEC JTC1/SC38 at http://www.iso.org/iso/iso_technical_committee.html?commid=601355 and http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=63902

4.3.2 European Commission Expert group on Cloud Computing Contracts

This is a European Commission initiative from DG Justice that deals with terms and conditions in cloud computing contracts between service providers and consumers and small firms.[68] The task of this group is supposed to be complementary to the work on model terms by the Cloud Select Industry Group on SLAs,[69] although its membership is different,[70] and its focus is slightly different because it is concentrating on the needs of the smaller cloud customer. To date, it has not published any comprehensive recommendations.

4.3.3 European Research projects on SLAs

In addition to the policy initiatives, there is a range of EU-funded research projects concentrating on SLAs for Cloud. These include: a study on standards terms and performance criteria in SLA for cloud computing services, that includes a model SLA[71]; a project called 'SLA-ready' that builds an SLA model that allows existing SLAs to be compared and to support SMEs in analysing their legal and organizational and technical needs for cloud[72]; a project called SLALOM that aims to create a set of cloud computing contracts covering all aspects of their relationship between a provider an adopter, but that includes SLAs.[73] DG Connect in the European Commission coordinates these research projects and hosted a workshop with participants from all projects on 11 May 2015.[74]

---

[68] Commission Decision of 18 June 2013 on setting up the Commission expert group on cloud computing contracts (2013/C 174/04), OJ C174/6, 20.06.2013. "Commission Decision expert group 2013).

[69] Commission Decision expert group 2013, recital 5.

[70] Commission Decision expert group 2013, art. 5. Its members include experts on data protection relevant to cloud computing, European and national umbrella organisations, business providing cloud computing services, representatives of cloud computing customers, representatives of the legal profession and academia and representatives of the European Commission. See the Commission Register of Expert Groups accessed at: http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailPDF&groupID=2922

[71] This research is carried out by Time.lex and Spark Legal Network & Consultancy and included a stakeholder workshop on 11 May 2015 to discuss cloud SLAs described at http://www.sparklegalnetwork.eu/dg-cnect-study-on-cloud-computing-slas-stakeholder-workshop-yesterday

[72] This project is described at http://www.sla-ready.eu/

[73] Information on this project is available at http://slalom-project.eu/sites/slalom/files/content-files/pages/SLALOM_Handout.pdf

[74] The minutes from the workshop have not yet been published but this link provides the invitation and the agenda for the meeting and participants at http://www.sla-ready.eu/sites/default/files/Workshop%20invitation_FINAL.pdf

4.3.4 International standards work on SLAs

The International Standards Organisation ISO/IEC JTC 1 Working Group on Cloud Computing is currently working on an international standard for Cloud SLAs.[75] The A4 Cloud project has contributed input to the SLA standardization document and work on this is on-going.

4.4 Cloud SLA survey 2015

This section describes and analyses the results for the survey of Cloud SLA's conducted as part of this Deliverable. It explains how the survey was conducted, the content of the SLAs, and the how this corresponds with the regulatory initiatives and models on cloud SLA standardisation.

4.4.1 Methodology used for choosing the SLAs for survey 2015.

In order to maintain consistency with past and future surveys, we studied only those SLAs which were offered by Cloud Providers included in the terms and conditions survey. It is possible that those Providers might offer SLAs to major customers as part of a negotiated contract, but again to allow for future surveys we examined only those SLAs which were publicly available on the website of the Cloud Service Provider. In total, 15 SLAs were examined, from 10 different Cloud Providers. This is less than the 30 terms of service surveyed but some services, particularly services that were focussed towards end users and free services, did not have SLAs.

The services that had SLAs were paying services with a focus on business users generally. The list of the SLAs surveyed and the Cloud Service Provider is given below.

Cloud Provider	***Service***	***SLAs***
CenturyLink	Savvisdirect[76]	* CloudStorage service SLA * SaaS Marketplace Applications SLA * Management Console SLA

[75] ISO/IEC JTC1/SC38 at http://www.iso.org/iso/iso_technical_committee.html?commid=601355 and http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=63902
[76] SLAs available at https://apps.centurylink.com/slas last accessed on 8 June 2015

Amazon	Amazon Web Services	* Cloud Front SLA[77] * Simple Storage Service S3[78]
ElasticHosts	ElasticHosts Cloud	Elastichosts Terms of Service including SLA[79]
GoGrid	GoGrid	* ServePath SLA[80] * ColoServe SLA[81] * 10,000% guaranteed SLA[82]
Google	GoogleApps for Business	GoogleApps SLA[83]
IBM	Smart Cloud	IBM SmartCloud (SaaS)[84]
Joyent	Joyent Cloud	Cloud Hosting SLA[85]
Rackspace	Rackspace Cloud Services	Managed Cloud Support[86]
Softlayer	Softlayer	Softlayer SLA[87]

[77] SLA available at http://aws.amazon.com/cloudfront/sla/ last accessed on 8 June 2015.
[78] SLA available at http://aws.amazon.com/s3/sla/ last accessed on 8 June 2015.
[79] SLA available at http://www.elastichosts.com/cloud-servers/terms-of-service/ last accessed on 8 June 2015.
[80] SLA available at http://www.gogrid.com/legal/servepath-service-level-agreement
[81] http://www.gogrid.com/legal/coloserve-service-level-agreement last accessed on 8 June 2015.
[82] SLA available at http://www.gogrid.com/legal/service-level-agreement-sla last accessed on 8 June 2015.
[83] Available at http://www.google.com/apps/intl/en-GB/terms/sla.html last accessed on 8 June 2015.
[84] Available at http://www.google.com/search?client=safari&rls=en&q=ibm+smartcloud+saas+sla&ie=UTF-8&oe=UTF-8 last accessed on 8 June 2015.
[85] Available at https://www.joyent.com/about/policies/cloud-hosting-service-level-agreement last accessed on 8 June 2015.
[86] Available at http://www.rackspace.co.uk/legal/managed-cloud-sla last accessed on 8 June 2015.
[87] Available at http://static.softlayer.com/SoftLayer4/pdfs/sla.pdf last accessed on 8 June 2015.

Dell	DellvCloud	SLA for Dell Cloud with VMware vCloud[88]

4.4.2 Description of content of SLAs

The SLAs are all quite short documents. Most SLAs are no more than 2-3 pages in length. All of them deal almost exclusively with service availability or service uptime. They generally follow the same format:

* Service Commitment - they contain a service commitment to make the service available for a certain percentage of time. This monthly service level is given as a target rather than a commitment, to reduce the risk of liability if it is not met. For example in the Amazon CloudFront SLA they provide that "AWS will use commercially reasonable efforts to make Amazon Cloud Front available with a Monthly Uptime Percentage (defined as calculated by subtracting from 100% the average of the Error Rates from each 5 minute period in the monthly billing cycle) of at least 99.9% during any monthly billing cycle."[89]

* Service Credit - SLAs normally have a section or clause dealing with the service credit. This means that for any period of unavailability below the target the customer receives a credit on the monthly fee. In some cases the credit is based on 5% of the monthly free for each 30 minutes of downtime per month. Normally the service credit is capped at a certain amount, and in most cases cannot exceed the monthly fee. In the Google Apps SLA it has a definition of Service Credit as a table giving the Monthly Uptime Percentage and 'the days of service added to the end of the service term (or monetary credit equal to the value of days of service for monthly postpay billing customers) at no charge to customers.'[90] For example, this gives 3 days for monthly uptime percentages between 99.9% and 99% and 15 days for monthly uptime percentages less than 95%.

* Limitations and exclusions – The SLAs all contain a number of exceptions to the service credit, notably for force majeure, for scheduled and emergency maintenance and for

[88] Available at https://www.scalematrix.com/dell/sla/ last accessed on 8 June 2015.
[89] 'Service Commitment' clause (unnumbered) in SLA available at http://aws.amazon.com/cloudfront/sla/ last accessed on 8 June 2015.
[90] "Service Credit' clause (unnumbered) in SLA available atAvailable at http://www.google.com/apps/intl/en-GB/terms/sla.html last accessed on 8 June 2015.

service interruptions caused by customer or third party equipment not within the control of the Cloud Service Provider.

All SLAs are subject to the terms in the Terms of Service or are said to be part of the service agreement even though they are in a separate document. For example, Rackspace provided "This Support SLA (the "SLA") is part of the Agreement for Managed Infrastructure and Managed Operations customers only and is subject to the terms of the Agreement."[91]
In terms of format, only one of the SLAs was actually in the same document as the Terms of Service,[92] the SLA for Elastichosts. It covered exactly the same matters as the other SLAs that were given as separate documents. It also gave a credit of the entire fee for the previous 30 days in the case of permanent loss of stored data, which was something that the other SLAs did not address.
The SLA for GoGrid was the most extensive in scope.[93] While the other SLAs only deal with service availability or uptime, GoGrid's SLA also addressed physical security, engineering support, cooling and environment, to name just a few of the additional areas where it gave performance and service undertakings.

SLAs – stronger and weaker than ToS

It is important here, particularly for non-lawyer readers, to emphasise that the obligations in SLAs are intended to be both weaker and stronger than obligations set out in terms and conditions. They are weaker because the only remedy for failure to achieve an SLA obligation is a partial refund of the service fee, in the form of a service credit.[94] Breach of obligations in the terms could in theory make the provider liable for all the customer's losses, though in practice that liability is limited severely by other terms. The SLA obligation is stronger because the remedy for breach is an automatic refund as specified in the service credit regime. Breach of a terms and conditions obligation will often be disputed by a provider, leading to negotiation of any remedy and as a last resort court action. Many breaches of terms and conditions

[91] First sentence in the SLA at http://www.rackspace.co.uk/legal/managed-cloud-sla last accessed on 8 June 2015.
[92] The SLA for Elastihosts available at http://www.elastichosts.com/cloud-servers/terms-of-service/ last accessed on 8 June 2015
[93] SLA available at http://www.gogrid.com/legal/service-level-agreement-sla last accessed on 8 June 2015.
[94] Typical language is: 'this is the sole and exclusive remedy for service interruptions, deficiencies or failure of any kind' (SavvisDirect: CloudStorage service SLA and SaaS Marketplace Applications SLA.). Similar wording is found in nearly all of the SLAs surveyed.

obligations will remain unremedied, whereas all breaches of SLA obligations should be compensated for.

4.5 SLAs – theory versus practice

The C-SIG guidelines on SLAs with the list of service level objectives produced by the European Commission gave an impressive range of possible SLOs that could be within the SLA. The unfortunate reality, based on the SLA survey 2015, is that the cloud service providers are currently giving SLAs that are very limited in scope, and just cover basic service availability. This gulf between the lofty expectations or guidelines and the rather disappointing reality has a number of possible explanations.

First, the guidelines are an aspirational ideal. They cannot be intended for use in all SLAs, and not all SLOs are appropriate for particular cloud relationships. Therefore, although the European Commission's SLOs are comprehensive and well explained, they are so extensive in scope that it would be very unlikely - at least for publicly available SLAs with standard term contracts – that any cloud service provider would offer all of these SLOs for a basic contract. The model or guidelines needs to be viewed as a 'pick and mix' that gives a range of SLOs that may be relevant to your industry, your contract or not at all.

Second, the survey dealt with publicly available SLAs from a range of services mainly aimed at smaller business users. This is the type of contract where the 'bare minimum' may be all that the Cloud Provider is commercially prepared to agree to; or where it does not want to make publicly available more detailed SLAs, perhaps for fear of advertising potential liability issues. It is more likely that the cloud service provider would be prepared to agree to a wider range of SLOs for bigger value, negotiated contracts, or at the request of a business user the cloud provider would make more a wider range of SLOs. The 'plain vanilla' SLO however, by default, is at present just about availability or 'uptime'.

Third, the current industry practice concerning cloud SLAs is that they are very limited in their scope. Industry commentators on cloud SLAs view cloud SLAs in a much more limited (or pragmatic?) way than those writing the model SLAs. The raison d'être for the cloud SLA, according to one commentator,[95] is that cloud carries risks that traditional IT did not – a greater

[95] Press article 'SLA Roundup' in Cloud Computing Insights (2014) available at http://www.cloudcomputinginsights.com/management/cloud-sla-roundup-rackspace-v-amazon-v-hp/?mode=featured

possibility of mass failure and service outage. For this reason, SLAs are a 'necessary thorn in the side of everyone involved in Cloud IT'.[96] Another jaundiced view of cloud SLAs is found in the many articles on cloud SLAs claiming that they are worthless.[97] For example, SLA credits as the only remedy for service outage rarely covers the losses that a customer would suffer, and the 100% uptime guarantees are just a marketing tactic since service credits only apply after 30 minutes or more of downtime. Some companies promise response times but not resolution times, thus offering customers no assurance that fixing a problem will be addressed with any urgency.

Fourth, business may be very reluctant to promise anything that could result in significant liability. Giving extensive SLOs, particularly on matters that could concern regulatory compliance (like data protection), could present the risk that service credits might eat up most of the provider's income stream in the event of an ongoing breach. Although the cloud service provider may want to build trust with the customer, by being open and transparent, they will not want to incur more liability.[98]

Fifth, the guidelines produced by C-SIG should be viewed as quasi-regulatory normative statements. Although produced in consultation with industry, they do not reflect the business reality of the SLAs that are on offer to smaller business users, and probably even to larger enterprises. Therefore, they are not statements of current best practice but rather an aspirational standard, which might hopefully be attained at a future date.

For all the reasons given above, the range of SLOs that a cloud service provider will give to its customers is likely to be limited. The question is which SLOs are cloud service providers likely to give that would increase accountability? This is addressed in the next section.

4.6 Recommendations for accountability

An increased range of SLOs can improve accountability, as well as having all the other potential benefits identified above. However, providers are unlikely to offer mass-market SLAs that cover a wide range of matters because of the risks of increasing their liability as discussed above. Therefore, we need to identify the areas where cloud providers would be open to

[96] Ibid

[97] "Three reasons why your SLA is Worthless" by Jeff Huckaby,available at http://www.rackaid.com/blog/worthelss-sla/ and http://www.cloudedissues.com/post/80628942067/on-slash-cloud-podcast-6-we-look-at-the-question

[98] For a detailed examination of liability issues see D-4.12, 'A4Cloud Tools Liability and Compliance Investigations'.

offering SLOs. Research on negotiated cloud contracts,[99] where cloud providers and customers negotiate the contract terms rather than accept standard terms of service, provides a useful starting point because it tells us the kinds of areas where cloud providers are open to negotiate and what areas they will not negotiate. This research indicates, by inference, what types of SLOs might be acceptable to cloud providers. If cloud providers are prepared to negotiate a term they must also be prepared to agree to certain actions and to define their performance, and this is the essence of an SLO.

In the negotiated contracts research, the findings were that certain terms were non-negotiable. Terms relating to liability, for example, exclusion of liability or limits on liability and remedies for breach of warranty or indemnities, were the areas where cloud providers were least likely to negotiate.[100] The research found that cloud providers usually provided that liability was 'non-negotiable' and that even large users had difficulty getting cloud providers to accept additional liability.[101] Therefore, as predicted, these terms are not likely to feature in any SLO in a Cloud SLA.

In contrast, the research found that terms relating to availability, reliability, performance and capacities or throughput were negotiable commercial issues varying with user requirements and so open to negotiation in SLAs.[102] These types of terms are typical in SLAs and form the subject matter of the SLAs surveyed.

There were issues that were not as clear-cut. Cloud providers often refused to negotiate regulatory issues, such as data protection compliance.[103] Nevertheless, some issues relating to data handling, such as data retention or deletion and data portability, were issues that cloud providers were open to negotiate.[104] Therefore, issues about the process after contract termination of handing over data or deleting or porting data have the potential to be addressed in SLOs.

As regards negotiating security issues, this had a mixed response from cloud providers. They resisted negotiation about pre-contractual audits or accepting customer's security policies,

[99] W Kuan Hon, Christopher Millard and Ian Walden 'Negotiating Contracts for Cloud Services' in Millard (ed), *Cloud Computing Law* (OUP, Oxford 2013).
[100] Ibid, 80-82
[101] Ibid, 81
[102] Ibid, 83-84
[103] Ibid, 85-86
[104] Ibid, 97-99

mainly to avoid incurring additional liability.[105] However, cloud service providers were prepared to attain independent certification to objective industry standards for cloud-specific security compliance.[106] They refused to allow or negotiate on audit rights for customers for security breaches; but third party audits were acceptable as a possible solution to this problem.[107] Finally, although security breach notification was not automatically available to customers as part of the contract, some providers agreed after negotiation to notify customers promptly or breaches or losses.[108] Other providers, while not obliged to do so under contract, in practice notified customers of any breach. Some providers accepted additional obligations such as to use 'commercially reasonable efforts to monitor and detect breaches'.[109] This indicates that certification, third party audits, security breach notification and monitoring are areas where cloud providers could be willing to accept SLOs.

In conclusion, based on the above, it appears that there are only a limited number of areas that cloud providers would be willing or likely to provide SLOs. These areas are about commercial matters, such as availability, reliability and performance of the cloud service, or about pure data handling, monitoring, logging and data retention. Areas that potentially concern liability or regulatory issues are likely to be non-negotiable. Therefore our recommendations are based on those SLOs that CSPs are likely to accept and that are most important from the point of view of accountability.

First, the most important recommendation for accountability purposes would be to advocate the inclusion in the SLA of an SLO on data breach notification policy, that sets out a procedure for establishing and notifying customers about personal data breach. This SLO is one of the recommended Data Protection SLOs in the European Commission guidelines under the heading "Accountability".[110] By notifying customers of data breaches, it creates transparency about data breaches. It also means that cloud service providers are responsive to their customers and have to proactively monitor and log data breaches and notify customers. It allows both the cloud service provider and the customer to try to remedy the breach, by fixing or retrieving the lost data or trying to repair the loss. This SLO is important for accountability because it directly relates to the attributes of transparency, responsiveness, remediability and verifiability. The research on negotiated contracts above indicated that

[105] Ibid, 92-93
[106] Ibid, 94
[107] Ibid 95-96
[108] Ibid, 96
[109] Ibid, 97
[110] Guidelines, at 35

cloud service providers were open to notify customers promptly of security breaches or data losses.[111] Other providers accepted additional obligations such as to use 'commercially reasonable efforts to monitor and detect breaches'.[112] This indicates that cloud providers may be willing to accept SLOs concerning data breach notification, although they may be wary of incurring any regulatory liability for data breach.

Second, in order to investigate data breaches or security incidents, the cloud service provider needs reliable monitoring and logging mechanisms. Therefore SLOs concerning security incident reporting, logging and monitoring and auditing and security verification would support monitoring and detecting both data and security breaches.[113] These SLOs are related to the accountability attribute of verifiability since these are the means by which the evidence is produced to demonstrate accountability.

Finally, SLOs concerning data management, including data classification, data portability and data retention after the end of the contract,[114] are all areas that cloud service providers would be wiling to accept SLOs[115] and that are relevant to accountability. SLOs in these areas would increase transparency and responsiveness to customers and so would increase accountability.

[111] W Kuan Hon, Christopher Millard and Ian Walden 'Negotiating Contracts for Cloud Services' in Millard (ed), *Cloud Computing Law* (OUP, Oxford 2013), 96
[112] Ibid, 97
[113] Guidelines, 23-25 set out a set of SLOs concerning each of these matters.
[114] Guidelines section on Data Management SLOs, 44-50.
[115] W Kuan Hon, Christopher Millard and Ian Walden 'Negotiating Contracts for Cloud Services' in Millard (ed), *Cloud Computing Law* (OUP, Oxford 2013), 97-99

5 Analysis of research findings and recommendations

In this Deliverable, we have given the results of the survey of thirty cloud standard contract terms in 2015; we have compared these with the standard terms surveyed in 2013; we have analysed the evolution of accountability in standard cloud computing contracts based on this comparison. We have also surveyed and analysed SLAs related to the contracts surveyed in 2015.

Our conclusions are given below followed by an analysis and explanation of these conclusions.

5.1 Evolution in standard cloud contract terms

Our first findings concern the evolution in standard cloud contract terms. Many of the contract terms surveyed in 2015 appear to be very similar to the contract term surveyed in 2013. Our initial research finding in the February 2015 report was that there little evolution or variation in the contract terms over the two-year period. Our conclusion in this Deliverable is more nuanced.

At first glance, there appeared to be little variation in the standard cloud contract terms in 2015 compared to the contracts in 2013. This is true for the majority of the 20 standard clauses identified: for example, for the clauses relating to limitation of liability, the clause relating to acceptable use policy, and many other of the standard clauses surveyed there are no differences between the 2013 survey results and the 2015 survey results.

Nevertheless, there are two areas in which the standard clauses in terms of service have evolved that indicate a greater trend towards accountability. First, as regards regionalization of contracts, more cloud providers specify a region for the cloud contract. This is relevant to the applicable law for the contract and it is also relevant to data transfer to certain jurisdictions. The survey indicated that more cloud providers are offering regional variations of their cloud contracts and that they are stating explicitly whether the customer's data will be transferred outside the jurisdiction. Second, as regards data handling, the survey indicated cloud providers are more likely to address issues such as disclosure to law enforcement authorities, data deletion, and data transfer. The data privacy policies and terms of service have evolved in a

way that shows an increasing trend towards more transparency by some cloud providers and more awareness of the need to be accountable for personal data in the cloud.

These trends do not apply to all cloud providers and all contracts. Nevertheless, there is a trend towards more accountability by an increasing proportion of cloud providers.

5.2 Significance of SLAs to accountability attributes

Our second finding from this research concerns the significance of SLAs to accountability attributes. What has changed markedly since the survey in 2013 is the way in which regulators and standardization bodies are proposing standard or model contract terms and standardized SLAs for cloud. This is a noteworthy development in terms of future evolution of cloud contracts. Both in the EU and at international level, standardized SLAs for cloud are emerging.

The SLAs are more likely to contain obligations, called Service Level Objectives or SLOs, that are directly relevant to accountability attributes such as transparency, responsiveness and verifiability. Examples include SLOs relating to logging and monitoring, auditing and security verification, and support response times. For this reason, SLAs could have a special significance for demonstrating accountability by cloud service providers in the future. Moreover, SLAs relate to accountability because they specify the remedy available to customers in the event of service unavailability or service failure, and to achieve this must of course specify the performance the customer is entitled to expect.

Although service providers are increasingly offering SLOs, they are not offering to compensate their customers for losses caused by failure to achieve those obligations. Most of the SLAs surveyed made it very clear that the only remedy available was the service credits offered.

Much has been said concerning model SLAs as a mechanism for introducing more transparency and trust and consequently more accountability.[116] Model SLAs might achieve this in the long-term, but our survey shows that the current use by providers of SLAs is as a limited performance or availability guarantee and as a mechanism to award service credits. As

[116] In the C-SIG Guidelines on SLAs discussed above but also as part of this research project A4 Cloud see http://www.a4cloud.eu/Workshop-on-Accountability-and-SLA-management-for-the-cloud

explained in earlier sections of this document,[117] service providers might be open to following the suggestions in the Guidelines on Cloud SLA published C-SIG, by introducing clauses that deal with response times for breach, data loss and security measures. However, this is not the SLA model currently offered to small or medium sized business users.

The current status of SLAs is that they have limited relevance to accountability. Our 2015 survey results indicated that SLAs deal with service availability or 'uptime' nearly exclusively. But the fact that both international and regional bodies are trying to develop standard SLAs with SLOs relating to a wide range of issues may mean that in the future SLAs are far more significant in indicating and guaranteeing accountability by cloud service provider. We hope this 2015 survey will be useful for future research to map the evolution of cloud SLAs and accountability.

5.3 Analysis and explanation of changes

Our analysis identifies some positive trends that indicate that cloud service providers are increasingly aware that customers require more transparency as regards how their data is used by their cloud service provider. Although there is no revolution in cloud provider contract terms (for example, limitation of liability clauses), many cloud providers are adapting their standard contract to address data protection and security concerns.

Factors that may be influencing these changes include ccustomer pressure or expectations following increasing publicity about data breaches and security in the cloud. As the cloud market matures, customer demands and expectations in respect of security, privacy and accountability issues are likely to evolve and become more sophisticated.

The second factor that may be influencing the change is that EU and national authorities are adopting non-binding model terms that act as a model or template for the ideal cloud terms. The European Commission working with industry have produced model terms for SLAs, and some national regulators, such as CNIL, have produced model terms for cloud contracts. These initiatives, while they are non-binding on cloud service providers, are likely to have more and more influence particularly if there is take-up by leading cloud providers.

[117] Sections 4.5 and 4.6

The final factor that may be influencing these developments is the publicity surrounding the reform of the EU data protection framework. The European Commission's proposal for a General Data Protection Regulation (GDPR) released in 2012 puts data protection at the top of the EU policy agenda. The ensuing debates between the various EU institutions concerning adoption of the new GDPR, still unresolved, has meant that data protection in the EU has been discussed, debated and remained at the top of the legislative agenda. This may be a third factor to explain why cloud providers have more awareness about data protection and, consequently, define data handling obligations in their standard terms more clearly.

5.4 Recommendations arising from this research

A research outcome requested by research partners in A4 cloud[118] is to produce concrete research recommendations useful for other work packages in A4 Cloud, for example, recommendations for particular contractual clauses or highlighting 'missing' contract terms for accountability. For example, this could be relevant to the A4Cloud work package on standards[119] that inputs into ISO standardization for model clauses in SLAs. We have identified what could constitute 'best practice or recommendations' in our analysis of the 20 contract terms and in the SLA analysis. These recommendations are summarized in Appendix 1.

6 Conclusion

In this Deliverable, we have surveyed standard contracts and SLAs in 2015 to give qualitative and quantitative data about the evolution in cloud contract terms in relation to accountability. Our analysis of the survey results has produced some recommendations for accountable standard terms relevant to the work of other A4 Cloud partners and even perhaps with wider relevance outside the project.

Our conclusion is that although there is no revolution in cloud standard terms or SLAs, there is a trend towards more accountability about data protection and security matters by cloud providers. We anticipate that this trend will continue, in part due to the work of the EU, national regulators, industry and international bodies. New laws and regulations will couple with model cloud standard contracts and SLAs that address data handling by cloud providers. We anticipate that, driven by the cloud service provider's need to reassure their customers

[118] This formed part of the reviewer comments on the internal report in February 2015 that preceded this public Deliverable as part of this work package.
[119] A4 Cloud, work package A5 on cloud standards.

following news stories and negative publicity concerning data leaks, providers will focus more strongly on accountability, particularly but not exclusively in relation to data protection. If they adopt accountability as part of their values for dealing with customers' data in the cloud, cloud service providers will introduce more comprehensive SLAs, particularly in relation to data handling, and thus be more likely to win the trust of their customers for cloud services.

7 References

Bovens, M. (2007) 'Analysing and Assessing Accountability: A Conceptual Framework' European Law Journal, 13(4):447-468.

Bovens, M (2010) 'Two concepts of accountability: Accountability as a Virtue and as a Mechanism' Special Issue: Accountability and European Governance: West European Politics, 35(5) 946-967.

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

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

Gleeson and Walden, 'It's a jungle out there: standardisation and cloud' EJLT 2014

Hon W K and Millard C, 'Cloud Technologies and Services,' in (eds) Millard C, *Cloud Computing Law* (Oxford University Press 2013)

Siani Pearson, "Privacy, Security and Trust in Cloud Computing", Privacy and Security for Cloud Computing, S. Pearson and G. Yee (eds.), Computer Communications and Networks, Springer, pp. 3-42, 2013.

Rehab Alnemr, Siani Pearson, Ronald Leenes and Rodney Mhungu, COAT: Cloud Offerings Advisory Tool, Proc. CloudCom, IEEE, pp. 95-100, 2014.

Siani Pearson, Accountability in Cloud Service Provision Ecosystems, Secure IT Systems, LNCS, vol 8788, Springer, pp. 3-24, 2014.

8 TABLES & APPENDICES

Table 1

Table 1 Cloud Standard contracts surveyed in 2015.

Provider	Services	Type of service
37signalas	Basecamp[120]	Collaborative project management tool
CenturyLink	Savvisdirect [121]	Virtualized application hosting via IaaS
ADrive	ADrive[122]	File hosting and backup via SaaS
Akamai	Terra[123]	Web acceleration via IaaS distributed caching
Amazon	Amazon Web Services[124]	Virtualized application hosting and data storage via IaaS
Apple	iCloud [125]	Email filehosting and personal information management via SaaS
EMC	MozyHome/Mozypro[126]	File hosting and backup via SaaS
Dropbox	Dropbox[127]	File hosting and backup via SaaS
Elastichosts	ElasticHosts Cloud[128]	Application hosting via

[120] Basecamp 'Terms of Service' (undated) available at https://basecamp.com/terms and last accessed on 5 June 2015.
[121] SavvisDirect 'Terms and Conditions' (1 June 2015) available at https://apps.centurylink.com/terms-conditions and last accessed on 5 June 2015.
[122] ADrive 'Terms of Service' (5 January 2015) and available at http://www.adrive.com/terms and last accessed on 5 June 2015.
[123] Akamai 'Privacy and Other Policies' includes a range of policies that such as a privacy policy, a safe harbor agreement policy, an arbitration agreement, an acceptable use policy, copyright notices, and is available at http://www.akamai.com/html/policies/index.html and include a link to legal notices for EU countries which gives the contract details and address for the subsidiaries in the UK, Germany, France, and Spain at http://www.akamai.com/html/policies/europe_legal_notices.html last accessed on 5 June 2015.
[124] Amazon Web Service 'AWS Service Terms' (23 April 2015) and available at http://aws.amazon.com/service-terms/ and last accessed on 5 June 2015.
[125] Apple 'iCloud Terms and Conditions' (20 October 2014) and available at http://www.apple.com/legal/internet-services/icloud/en/terms.html and last accessed on 5 June 2015.
[126] Mozy by EMC 'Mozy Terms of Service' (11 June 2014) available at https://mozy.com/about/legal/terms and last accessed on 3 June 2015.
[127] Dropbox 'Dropbox Terms of Service' (1 May 2015) available at https://www.dropbox.com/terms and last accessed on 3 June 2015.
[128] Elastichosts 'Elastichosts Terms of Service, SLA & AUP' (undated) available at http://www.elastichosts.com/cloud-servers/terms-of-service/ and last accessed on 3 June 2015.

		IaaS
Facebook	Facebook[129]	Social networking (including application sharing) via SaaS
Flexiant	Flexiant Cloud Orchestrator[130]	Application Hosting via IaaS
GoGrid	GoGrid[131]	Virtualised application hosting and data storage via IaaS
Google	Google Apps for Business[132]	Application creating and hosting via PaaS
Google	Google Drive[133]	Document creation and sharing via SaaS
IBM	Cloud Managed Services[134]	Virtualised application hosting and data storage via IaaS
Joyent	Joyent Cloud[135]	Application hosting via IaaS
Microsoft	Windows Live & Onedrive[136]	Data sharing and sync via SaaS
PayPal	PayPal Services[137]	Payment and accounts handling via SaaS
Rackspace UK	Rackspace Cloud Servers[138]	Virtualised application hosting and data storage via IaaS

[129] Facebook 'Statement of Rights and Responsibilities ' (30 January 2015) available at https://www.facebook.com/legal/terms and last accessed 3 June 2015.
[130] Flexiant 'Terms of Use' (undated) available at https://www.flexiant.com/terms-of-use/ and 'Flexiant Cloud Orchestrator End User licence agreement' (undated) available at https://www.flexiant.com/support/eula/ and last accessed on 3 June 2015.
[131] GoGrid 'Terms of Service' (22 November 2013) available at http://www.gogrid.com/legal/terms-service and last accessed on 3 June 2015.
[132] Google 'Google Apps for Business (Online) Agreement' (28 March 2012) available at https://www.google.com/intx/en_in/work/apps/terms/2013/1/premier_terms.html and last accessed on 4 June 2015.
[133] Google ' Google Terms of Service' (14 April 2014) available at https://www.google.com/policies/terms/ and last accessed on 4 June 2015.
[134] IBM 'Cloud Services Agreement' (undated) available at http://www-05.ibm.com/support/operations/files/pdf/csa_us.pdf and last accessed on 4 June 2015.
[135] Joyent 'Terms of Service' (3 April 2014) available at https://www.joyent.com/about/policies/terms-of-service and last accessed on 4 June 2015.
[136] Microsoft 'Microsoft Services Agreement (31 July 2014) available at http://windows.microsoft.com/en-us/windows/microsoft-services-agreement and last accessed on 4 June 2015.
[137] PayPal 'User Agreement for PayPal Service' (15 April 2015) available at https://www.paypal.com/uk/webapps/mpp/ua/useragreement-full?locale.x=en_GB and last accessed on 5 June 2015.
[138] Rackspace 'Cloud Terms of Service' (13 November 2014) available at http://www.rackspace.com/information/legal/cloud/tos and last accessed on 5 June 2015.

Salesforce	Sales Cloud[139]	HR and CRM services via SaaS
Symantec	Norton Online Backup[140]	Backup via SaaS
Softlayer	Softlayer[141]	Virtualised application hosting and data storage via IaaS
UKFast	CloudHosts[142]	Application hosting via IaaS
Zoho	Zoho Services[143]	Document creation and sharing via SaaS
500px	500px[144]	Image hosting via SaaS
Box	Box Personal/Business[145]	Document creation and sharing via SaaS
Dell	DellvCloud[146]	Data Hosting via IaaS
Linux	Linode[147]	Virtual Server Hosting via IaaS
Oracle	Exalogic Elastic Cloud[148]	Virtual Server Hosting via IaaS
Mega	Mega[149]	Storage via SaaS
Canonical	Ubuntu One[150]	Storage via SaaS

[139] Salesforce 'Cloud Master Subscription Agreement' (1 September 2014) available at http://www.salesforce.com/company/legal/agreements.jsp and last accessed on 5 June 2015.
[140] Norton 'Norton Online Backup Terms of Service Agreement' (undated) available at https://nobu.backup.com/terms_of_service and last accessed on 5 June 2015.
[141] Softlayer 'Master Service Agreement' (March 2014) available at http://www.softlayer.com/legal and last accessed on 5 June 2014.
[142] Cloudhost 'Terms of Service' (undated) available at https://cloudhost.com.ng/terms.php and last accessed on 5 June 2015.
[143] Zoho 'Terms of Service' (19 April 2015) available at https://cloudhost.com.ng/terms.php and last accessed on 5 June 2015.
[144] 500px 'Terms' (9 August 2012) available at https://500px.com/terms and last accessed on 5 June 2015.
[145] Box 'Box Terms of Service' (4 August 2014) available at https://www.box.com/legal/termsofservice/GB/ and last accessed on 5 June 2015.
[146] Dell 'Commercial Terms of Sale' (undated) available at http://www.dell.com/learn/uk/en/ukcorp1/solutions/art-commercial-terms-of-sale-uk?c=uk&l=en&s=corp&cs=ukcorp1 and last accessed on 5 June 2015.
[147] Linode 'Terms of Service' (undated) available at https://www.linode.com/tos and last accessed on 5 June 2015.
[148] Oracle 'Oracle Online Cloud Services Agreement' (undated) available at http://www.oracle.com/us/corporate/contracts/cloud-csa-uk-en-2352082.pdf and last accessed on 26 June 2015.
[149] Mega 'Mega Limited Terms of Service' (undated) available at https://mega.co.nz/ios_terms.html and last accessed on 5 June 2015.
[150] Canonical ' Ubuntu One Terms of Services' (January 2014) available at https://login.ubuntu.com/terms/ and last accessed on 5 June 2015.

Table 2

Table of 20 contract terms surveyed in 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 authorities 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.

Appendix 1

Best practice for cloud terms for greater accountability

These recommendations are based on our analysis of the 20 contract terms in our survey. These indicate the types of term that represent best practice or recommended practice for accountability. Some terms were found to be irrelevant to accountability and so there are no recommendations on accountability.

Term	What it means in a cloud contract	Best practice for accountability
Applicable law	Clause setting out the relevant law for interpreting the terms in the contract	The cloud provider offers a choice of law that relates to the place of residence or business address of the customer.
Jurisdiction	Clause setting out the court where any disputes over the contract will be held	The cloud provider offers a jurisdiction clause that relates to the place of residence or business address of the customer.
Arbitration	Clause providing that disputes will be resolved by arbitration rather than litigation	Arbitration clauses that give the choice of arbitration to the customer and do not seek to impose it on customers for all disputes.
Acceptable Use	Clause or policy defining what the provider considers as acceptable use of the cloud service	No recommendation.
Variation of contract terms	Clause permitting variation of contract terms by the service provider, often unilaterally.	Clause varying contract terms by giving the customer advance notice of major contract changes by emailing or otherwise contacting customer directly about proposed contract changes (rather than just posting changes on the cloud service provider's website). Customers may chose 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.
Data integrity	Clause putting the responsibility for ensuring the confidentiality and integrity of personal data onto the customer and not the cloud provider	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.
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	The cloud service provider 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. The cloud provider should undertake to guarantee the easy portability or reversibility of customer data in a structured and widely used format.
Data disclosure	Clause setting out the circumstances in which providers will, or may, disclose customer information to law enforcement authorities and courts	The cloud provider states explicitly the circumstances in which it will disclose information to law enforcement authorities (LEAs) or not. When it reserves discretion to notify LEAs itself, it should also undertake to let the customer know that disclosure has taken place as soon as reasonably practicable.
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)	The cloud service provider states where it will store and transfer data, whether by reference to particular regions or worldwide. A clause should undertake to adhere to data protection principles in storing and

		transferring data and, where relevant, the safe harbor principle. In the event that the CSP reserves the right to transfer data outside of the EEA, it could undertake to notify customers when it does so.
Monitoring by provider	Clause describing if and how the cloud service provider will monitor the customer's use of the cloud service	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 it is doing so (for example, service quality or technical performance or compliance with the acceptable use policy or other purposes).
IP Rights over service or content	Clause asserting IP rights over content and data uploaded to the cloud by customers	No recommendation – not applicable.
Proprietary rights and duties	Clause asserting ownership of data stored in or processed via the cloud provider services	No recommendation – not applicable
Warranty	The warranty or guarantee given by the service provider to the customer for the performance of the service	Clauses limiting warranties or guarantees should be proportionate and not exclude all liability in all circumstances. Otherwise they are not accountable by denying the customer a remedy even when the cloud provider is in breach of contract.
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	Clauses limiting direct liability should be proportionate and not exclude all liability in all circumstances. Otherwise they are not accountable by denying the customer a remedy even when the cloud provider is directly responsible for the damage or contract breach.

Indirect liability	Clauses concerning liability for indirect, consequential, or economic losses arising from a breach by the cloud provider	No recommendation.
Limit of liability	Clause limiting the extent of any damages or compensation that the provider may be liable for breach	It should be made clear by cloud service providers that include a liability cap that these clauses do not apply to customers who are consumers.
Indemnification	Clause that indemnify the provider against any claim against the provider arising from the customer's use of the service	No recommendation – not applicable
Service availability	Clause that specify a service performance target by the cloud service providers	No recommendation – not applicable
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.	Our recommendation is to include such clauses since it is an efficient way of providing a remedy to customers for service failure without obliging the customer to bring a court case.
Terms of payment clause	Whether the contract has a periodic payment clause or not.	No recommendation – not applicable.