CLOUD ACCOUNTABILITY PROJECT

D:D-4.5 Report on Legal and Regulatory Dependencies: embedding accountability in the international legal framework

Deliverable Number:	**D-4.5**
Work Package:	**WP44**
Version:	**Final**
Deliverable Lead Organisation:	**QMUL**
Dissemination Level:	**PU**
Contractual Date of Delivery (release):	**31 December 2015**
Date of Delivery:	**17 December 2015**

Editor
Chris Reed (QMUL)

Contributors
Chris Reed (QMUL), Dimitra Stefanatou (TiU)

Reviewer(s)
Siani Pearson (HP), Frederic Gittler (HP)

Executive Summary

This Deliverable explains how the A4Cloud research findings on accountability might be embedded in the international legal framework, and makes suggestions as to how this might be achieved through the work of the United Nations Commission on International Trade Law (UNCITRAL) and the Organisation for Economic Cooperation and Development (OECD).

It begins by introducing the concept of accountability and the A4Cloud terminology adopted for the analysis in the text. Section 1 then continues by making the argument for attempting to embed accountability in legal instruments at the international level. We argue that if the aim is to achieve a global legal framework which is functionally equivalent in its effects in each country, the first step has to be to seek consensus about how cloud computing entities *ought* to behave, rather than attempting to persuade the world to adopt any particular set of detailed legal rules. In consequence, we propose that the starting point should be the development of recommendations and guidelines for cloud provider contracts, focusing on accountability, because this is an area where international consensus is likely to be achievable and because there are important organisations, primarily UNCITRAL and the OECD, which could lead this work.

Section 2 explains the concept of accountability in more detail, focusing on how it might apply to cloud providers and their contracts. It uses the findings of Workstream C, and explains how the five main Accountability Attributes (transparency, responsiveness, responsibility, remediability and verifiability) can be translated at a high level into desired provider behaviours which can be captured in recommendations and guidelines.

Section 3 then attempts a first draft of an appropriate set of recommendations and guidelines, accompanied by explanatory commentary. These are arranged analytically according to the Accountability Attributes, to show how different aspects of commonly regulated behaviour (such as information disclosure and data security) can be addressed in order to achieve each attribute. A layered model is adopted, following the analytical approach of Workstream C, indicating how the development of recommendations and guidelines over time might address provider contractual behaviour in increasing detail. At the lowest level, examples are given about how the terms of contractual agreements might deal with privacy and data protection issues so as to illustrate how the different focuses of UNCITRAL and the OECD might be coordinated.

Section 4 concludes by explaining the advantages of adopting a soft law approach, particularly in the light of what can realistically be expected from cloud providers and taking into account the fundamental differences between EU and US legal systems that cannot be fully mitigated through the adoption of an international soft instrument governing the cloud. It briefly discusses some of the challenges which would need to be addressed when moving from an international soft law consensus to specific national legal implementations.

As important and useful background, Appendix 1 explains the current state of the most significant cloud-relevant legislative developments and other related initiatives in Europe and beyond. Progress towards finalisation of the General Data Protection Regulation (GDPR) is summarised, and the difficulties which are likely to arise from the decision of the Court of Justice of the European Union in *Maximillian Schrems v Data Protection Commissioner* are explained, as is the current state of the consequential negotiations towards agreeing modification to the EU/US Safe Harbor Agreements. We conclude that although these matters are due to be resolved initially in early 2016, the long-term incompatibility between the EU and US positions will continue to create uncertainty for some years. The state of play in pursuing the European Commission's cybersecurity strategy is also described.

Appendix 2 discusses the difficulties of reaching consensus and producing an internationally binding instrument. It sets out road map for this embedding, describing the likely process, from initial, high-level recommendations and guidelines through to (potentially) a binding international Convention. It

expands on the argument in the main text that the focus at this stage should be on high-level work to secure agreement on the general framework for embedding accountability, because an attempt to produce agreement at a detailed level is likely to be too controversial at this stage for any likelihood of success.

Appendix 2 also identifies a number of foundational issues, principles which should be adhered to so far as possible so as to make it more likely that the reforms will actually achieve their objectives, and to assist in reducing conflict with other laws. Some of these are agreed to be relevant to all information technology laws – technology neutrality, recognising the special position of intermediaries via liability immunities, consumer protection, data portability and data security. We also propose a cloud-specific foundational principle - that the primary responsibility for achieving legal compliance in cloud computing in respect of how data is handled should be placed on the cloud customer, and that whether a similar responsibility should be imposed on the cloud provider is a matter to be left to national law and/or contracts between cloud provider and customer. Our reasoning is this enables recommendations and guidelines to concentrate on the core of agreement internationally, leaving questions of wider responsibility to nation states and thus deferring their discussion to a later stage of the process.

Table of Contents

Executive Summary 2

Final Report on Legal and Regulatory Dependencies – embedding accountability in the international legal framework 5

1 Introduction 5

1.1 Concepts and Terminology 5

1.2 The International Framework 6

1.3 Structure of the Deliverable 7

2 Accountability and Cloud Providers 8

3 Cloud Computing Contracts – recommendations and guidelines 10

3.1 Transparency 12

3.2 Responsiveness 15

3.3 Responsibility 16

3.4 Remediability 17

3.5 Verifiability 19

4 Conclusions 20

Appendices 22

1 Related legislative and soft law initiatives 22

1.1 Progress on the EU Legislative Framework 22

1.2 Other Cloud Relevant Initiatives 24

2 A Road Map for Embedding Accountability 26

2.1 The Road Map 26

2.2 Scope 27

2.3 Foundational Principles 29

Select Bibliography 34

Final Report on Legal and Regulatory Dependencies – embedding accountability in the international legal framework

1 Introduction

As originally envisaged in the A4Cloud Description of Work, this deliverable was to constitute the final report on the legal and regulatory dependencies for effective accountability and governance, covering relevant legal and regulatory developments, with a particular focus on the proposed European Union (EU) data protection legislation and global initiatives relating to accountability in the cloud. An underlying assumption was that the EU General Data Protection Regulation (GDPR[1]) would by now have been enacted some time ago, so that this Deliverable would be able to discuss issues of implementation and review any other legal and regulatory developments which would be helpful in guiding the final development of the A4Cloud toolset. However, the GDPR proved more controversial than had originally been anticipated, although a final text has been agreed but not yet ratified at the time of writing.[2]

A decision was therefore taken, after consultation with the Advisory Board and the project reviewers that this deliverable would instead focus on the future impact which the A4Cloud project might have on law and regulation. At this stage of legal development, and given the wide range of cloud-relevant initiatives launched by different bodies, it seems a timely moment to explore how the project's finding might be embedded in a legal framework suitable both for the EU and beyond, particularly as there is a wide range of cloud-relevant initiatives at the EU, nation-state and transnational level which would benefit from such an approach.

Thus, building on the project findings so far, this deliverable expands on how a framework could be developed at an international level which is suitable to promote accountability in relation to data, particularly personal dat, processed in the cloud.

1.1 Concepts and Terminology

An initial difficulty is that there is no clear and uniform understanding of the concept of accountability. The range of views is particularly wide where handling of personal information is concerned, the major focus of the A4Cloud project:

> *Views differ on what 'accountability' involves. Article 29 Data Protection Working Party, Opinion 1/2010 on the principle of accountability, WP 173 (2010) seems to consider that 'accountability' involves taking measures to enable compliance with the data protection requirements and being able to demonstrate that that has been done. In contrast, the broader PIPEDA [Canadian Personal Information Protection and Electronic Documents Act 2000] approach treats accountability as end-to-end responsibility on the part of the controller; for instance, there is no prohibition on transfer of personal data abroad, but the controller remains accountable for the data wherever it is held – PIPEDA sch 1, 4.1.3.*[3]

[1] See notes 36 to 38 for references to the different texts of the proposal.
[2] http://europa.eu/rapid/press-release_IP-15-6321_en.htm. See Appendix 1.1 for further discussion.
[3] Hon, W. Kuan and Millard, Christopher and Walden, Ian, Who is Responsible for 'Personal Data' in Cloud Computing? The Cloud of Unknowing, Part 2 (March 21, 2011). International Data Privacy Law (2012) 2 (1): 3-18; Queen Mary School of Law Legal Studies Research Paper No. 77/2011. Available at SSRN: http://ssrn.com/abstract=1794130.

One of the main aims of A4Cloud was to bring clarity to this area, and so this deliverable adopts the formulation of the concept developed by Workstream C,[4] as explained further in section 2. In summary, accountability consists of an actor providing an account in the form of a report or description of an event or process, in which the accounting actor explains what has occurred and how, its reasons, and what will or could be done to remedy the situation and prevent its reoccurrence.

Terminology is also an issue, with the entities potentially involved in cloud accountability relationships being labelled differently depending on a particular author's preferences. For consistency we adopt the Workstream C terminology:[5]

> 1. **Cloud Subject:** An entity whose data are processed by a cloud provider, either directly or indirectly …
>
> 2. **Cloud Customer:** An entity that (a) maintains a business relationship with, and (b) uses services from a Cloud Provider …
>
> 3. **Cloud Provider:** An entity responsible for making a [cloud] service available to Cloud Customers

The taxonomy contains other cloud players, but for the purposes of the discussion to follow only the first three are considered.

It is important to note here that a single entity might play more than one role; for example, a provider who uses sub-providers will occupy the role of Cloud Customer in its relations with each sub-provider, and similarly a customer which processes its own data will also be a Cloud Subject in its relations with others in the cloud infrastructure. Law and regulation deal with this problem by applying at the level of the role, not at the level of the entity. Thus, as an entity changes roles, different legal and regulatory regimes apply to its activities.

1.2 The International Framework

Accountability is important globally, not just at a national level. Cloud computing is a global activity, and thus any substantial national differences in the legal and regulatory environment present major barriers to the adoption and use of cloud. This suggests that A4Cloud should seek to influence developments at the international level, in an attempt to have global impact.

An important reason for focusing this work at the international level, rather than at national law, is the diversity of legal and cultural approaches to the issues which accountability raises. Because of these differences, it is notoriously difficult to transplant a law devised in one legal tradition to a country which has a different tradition. By working instead from general principles, endorsed internationally, it is potentially possible to achieve a global legal framework which is functionally equivalent in its effects, at best by enrolling cloud providers as positive agents committed to the achievement of the regulatory aims through their own efforts rather than forcing them to comply through sanctions. The aim is to achieve agreement on what lawyers describe as the 'normative' content of law and regulation, ie statements describing how entities *ought* to behave.[6] At this stage of development, decisions about how entities *shall* or *must* behave in order comply with these statements need to be left to their implementation by

[4] Felici, M., Pearson, S. (eds.): D:C-2.1 *Report detailing conceptual framework*. Deliverable D32.1, Version Final, A4CLOUD (2014).

[5] Ibid, 23.

[6] The distinction in legal analysis between mere norms and legal rules is of fundamental importance – see HLA Hart, *The Concept of Law* (2nd, Oxford: Oxford University Press 1994).

nation-states, so that account can be taken of those states' particular legal, political and cultural traditions.[7] To avoid confusion between the legal usage of the term 'normative' and usages in other fields, we will instead invent the term 'behaviour-shaping'.

However, the law relating to cloud computing is not yet in a state where it is feasible to produce a detailed instrument which sets out the imperative rules which entities must follow. Presently there is not even any consensus on the areas of law and regulation which apply to cloud computing and might require approximation globally. Because these areas have not been identified, there is obviously a long way to go before the world can reach any consensus about the necessary content of law and regulation. It is also important to recognise that cloud computing technology is evolving so rapidly, as are the business models for its exploitation, that any international instrument would rapidly become out of date, most probably even before its text was finalised. Thus no purpose can be served by attempting to draft a Convention on cloud computing law and accountability. We must begin at the beginning.

For this reason, there is no attempt in what follows to build in those elements of the GDPR which have specific relevance for accountability. These elements are at far too specific a level for this early stage of international consensus building. Further, there are real difficulties in reconciling the GDPR with the activities of law enforcement and security agencies, particularly in relation to the United States (US) Safe Harbor scheme, as explained in Appendix 1.1, which raises questions as to whether the EU data protection regime will need further modification in the near future.

Instead, we propose that the process of building an international consensus on the behaviour-shaping statements which embed accountability in law and regulation should begin with guidelines and recommendations for cloud computing contracts. This is an area which has already received attention at the international level, as discussed in Appendix 1.2, and where there is, in our view, a genuine prospect of success.

Another reason why the international level is worth addressing is that there are influential transnational organisations who have a track record of successfully initiating and guiding the development of global legal norms. Appendix 2 discusses two of these organisations, the UN Commission on International Trade Law (UNCITRAL) and the Organisation for Economic Co-operation and Development (OECD), and explains the role they might play in embedding accountability.

1.3 Structure of the Deliverable

Section 2 explains the concept of accountability in more detail, focusing on how it might apply to cloud providers. Section 3 makes behaviour-shaping recommendations as to how cloud service providers should best promote accountability through the terms of their contractual agreements, including specific recommendations relating to privacy and data protection which are appropriate to be dealt with at this stage. Section 4 concludes by explaining the advantages of adopting a soft law approach, particularly in the light of what can be realistically be expected from cloud providers and taking into account the fundamental differences between EU and US legal systems that cannot be fully mitigated through the adoption of an international soft instrument governing the cloud; it concludes with an explanation of the most important challenges which would need to be addressed when moving from an international soft law consensus to specific national legal implementations.

As important and useful background, Appendix 1 explains the current state of the most significant cloud-relevant legislative developments and other related initiatives in Europe and beyond. Appendix 2 expands on the difficulties of reaching consensus and producing an internationally binding instrument, discussing the likely process involved and explaining the reasons why a choice was made in the context of the present analysis to consider soft law, in the form of recommendations and guidelines, as the most

[7] See Appendix 2.3 for a discussion of some of these differences.

appropriate means to initiate the process of regulating how companies should behave when providing services through the cloud.

2 Accountability and Cloud Providers

Accountability is a much-used term, but is often used without clear definition of what it is intended to mean. For this reason, an important element of the A4Cloud research has been to identify and clarify the meaning of the concept and explain how it can be applied to cloud computing. This work is set out in Deliverable C-2.1, *Report detailing conceptual framework*.

At the core of this work is the concept of an *account*, which is a description of what has occurred and an explanation of the reasons and how the accountable actor might change its behaviour for the future:

> … it is suggested that an account, when required and/or provided, should mean the accountable actor providing a report or description of an event or process … Ultimately, the account, while contextually and factually dependent, should generally include the answers to what are traditionally referred to as the 'reporters' questions', i.e. who, what, where, when, why and how, backed up with as much evidence as possible to validate the account. Often an account will also include the measures being taken to remedy a breach or failure and to prevent such breaches or failures in the future.[8]

The C-2.1 Report defines a multi-layer model of accountability. At the abstract level it is defined in terms of Accountability Attributes, which are 'conceptual elements of accountability applicable across different domains'. These attributes are implemented or operationalised via Accountability Practices, which describe the forms of behaviour which an accountable organisation will exhibit. Those practices will employ Accountability Mechanisms, a toolbox of organisational processes, controls, relationships and technical tools, which in combination achieve the implementation of the Accountability Practices in operational terms.

For the purposes of this deliverable we will focus on the Accountability Attributes as our basis for developing transnational guidelines and recommendations which embed accountability into cloud contracts and the privacy practices of cloud providers. Accountability Mechanisms, and to a lesser extent Accountability Practices are context-dependent, and so will vary between organisations because they have different business and operational models and use different technologies. Law and regulation need to have general application, and so must be derived from the abstract layer of the model. It is also important to recognise that this Deliverable focuses on the very earliest stage of developing transnational guidelines and recommendations; the securing of agreement on the fundamental principles which each nation state's law should reflect. Only once that agreement has been reached is it possible to focus in more depth about, for example, the details of what a cloud provider should do in terms of transparency or privacy protection.

There are five core Accountability Attributes:[9]

> **Transparency**: the property of a system, organisation or individual of providing visibility of its governing norms, behaviour and compliance of behaviour to the norms.

[8] Massimo Felici and Siani Pearson (eds), *Report detailing conceptual framework* (2014 FP7 A4Cloud project deliverable C-2.1) 19.
[9] Ibid, 32-3.

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.

Currently much of what happens in cloud computing is completely opaque to customers and other outsiders – thus the term 'cloud'. Transparency requires cloud providers to disclose the information which customers need if they are to make an appropriate choice of cloud service. It also requires disclosure of the information needed by customers during service operation, so that those customers can meet the obligations they owe to cloud users and to third parties such as regulators.

> **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 relationship between cloud providers and 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 be involved with the process by which the account is produced, and not only with the product.

It will be important here to distinguish the need for responsiveness from the mechanisms by which an obligation to respond is imposed. Whilst consensus might be achievable about when a response is needed and what its contents might be, national lawmakers will want to resort to different mechanisms to achieve the response. Some might wish to impose response obligations directly by law, whereas others might be content to leave this matter to the provider/customer contract.

> **Responsibility:** the property of an organisation or individual in relation to an object, processor 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 needs to be identified.

Responsibility, in the A4Cloud taxonomy, is not equivalent to liability. Rather, it refers to the actions which an organisation ought to undertake in response to problems arising (eg a data security breach). As with responsiveness, we must distinguish between responsiveness obligations and the legal mechanisms by which those obligations are imposed.

> **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 is not sufficient on its own. Further action is required in order to be accountable. Such action might include accepting legal responsibility, usually in the form of liability to compensate for loss, but accountability equally puts emphasis not only on whom to blame but how to repair the damage.

This latter point is important, because lawyers have a natural tendency to focus on liability (in terms of compensation or punishment) and thus ignore other ways in which a satisfactory remedy might be offered. Guidelines and recommendation in the fields of cloud contracts and data privacy need to focus on both.

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. Verifiability is important because accountability requires both the defining and displaying of relevant norms, and behaviour which demonstrates compliance with those norms.

The focus here would primarily be on mechanisms for providing such verifiability, rather than on legal obligations to do so (though legal obligations will of course form a part). Providing verifiability is particularly a technical challenge, and a large part of A4Cloud's work has consisted in researching tools which can assist in providing verifiability. Thus recommendations and guidelines might impose obligations to provide verifiability, but will most appropriately leave the devising of those mechanisms to accountable organisations.

Because the Accountability Attributes are expressed at an abstract level it is far from obvious how they might be implemented in law and regulation. What is required is a translation from attributes into what might be described as legal and regulatory Accountability Practices, and this is what Section 3 attempts.

3 Cloud Computing Contracts – recommendations and guidelines

We have argued earlier that producing recommendations and guidelines for cloud provider contracts with their customers is the most effective starting point for building an international consensus. But lawmakers and regulators in some countries have expended substantial effort in devising detailed rules for how processors of data should behave, particularly in relation to privacy and data protection. It is reasonable for them to ask why these rules are not incorporated in the recommendations and guidelines set out in this Section. There are two answers to this question.

The first is that no national or regional lawmaker has convinced the entire world of the correct approach to privacy and data protection. This means that incorporating the detailed rules of any particular law system is unlikely to achieve consensus between states which prefer a different approach to the problem. This difficulty has been recognised in the work of the Asia Pacific Economic Cooperation (APEC) in its 2005 Privacy Framework.[10] The APEC member nations are divergent in their legal traditions and their current approaches to privacy, and so to achieve a consensus between them the Preamble of the APEC Guidelines explains that their distinctive approach is to:

> *… focus attention on practical and consistent information privacy protection … it balances information privacy with business needs and commercial interests, and at the same time, accords due recognition to cultural and other diversities that exist within member economies.*

APEC therefore focuses not just on the privacy interests of individuals, which would include cloud subjects, but goes further and attempts a balancing exercise between those interests and business and commercial interests. This is seen as essential because companies are the entities who exercise practical control over the trans-border data flows on which the Privacy Framework focuses, and who therefore have to implement privacy-preserving measures. Once states agree on the basic responsibilities of such companies, it can be left to the companies to devise implementation measures which are appropriate to their business activities, in the light of whatever detailed regulation and sanctions each state implements. This is seen particularly clearly in paragraph 26, which specifically embeds accountability into the Framework:

> A personal information controller should be accountable for complying with measures that give effect to the Principles stated above. When personal information is to be transferred to

[10] APEC Privacy Framework, available at:http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx

> another person or organisation, whether domestically or internationally, the personal information controller should obtain the consent of the individual or exercise due diligence and take reasonable steps to ensure that the recipient person or organisation will protect the information consistently with these Principles.[11]

This requirement for 'due diligence' is far from an imperative rule, but in the context of a diverse international legal framework it is an effective means for the regulator to encourage companies to do their duty in a careful manner, to take care of the personal information entrusted to them, while giving them certain freedom as to how concretely to do so.

The second answer is that existing data protection and privacy laws do not, because of their historical origins, make full use of accountability. Lawmakers assert that they recognise accountability as an important component of privacy and data protection law, but a closer examination reveals that this is not entirely accurate. In relation to EU data protection law, the EU supervisory authorities (naturally perhaps) see accountability solely as a mechanism for securing and demonstrating compliance with the law, rather than as a value in its own right, and therefore concentrate on its responsibility and verifiability elements.[12] Principle 4 in Schedule 1 of Canada's Personal Information Protection and Electronic Documents Act 2000 specifically imposes accountability obligations on organisations and the individuals within those organisations, but those obligations are seen by the regulator primarily in terms of responsibility[13] and by the courts in terms of liability (remediability).[14] Transparency, often described as the primary element of accountability[15], is deal with randomly if at all.

In developing guidelines and recommendations for cloud provider contracts, we propose that the overriding aim should be that providers increase their level of accountability. This will improve the ability of cloud customers to achieve legal compliance, and might in time lead the market to demand enhancements to services for that purpose. There is a real danger that if accountability obligations are enumerated and elaborated in legislation they become set in stone, so that even if there were the technical ability to provide more accountability, no market for it would develop because of the legislation. As an example, in the related field of e-signatures there is a strong argument that the EU e-Signatures

[11] According to a short commentary on accountability provided in the text of the APEC Privacy Framework:

> Efficient and cost effective business models often require information transfers between different types of organizations in different locations with varying relationships. When transferring information, personal information controllers should be accountable for ensuring that the recipient will protect the information consistently with these Principles when not obtaining consent. Thus, information controllers should take reasonable steps to ensure the information is protected, in accordance with these Principles, after it is transferred. However, there are certain situations where such due diligence may be impractical or impossible, for example, when there is no on-going relationship between the personal information controller and the third party to whom the information is disclosed. In these types of circumstances, personal information controllers may choose to use other means, such as obtaining consent, to assure that the information is being protected consistently with these Principles. However, in cases where disclosures are required by domestic law, the personal information controller would be relieved of any due diligence or consent obligations.

[12] Article 29 Working Party, Opinion 3/2010 on the principle of accountability (WP173, 13 July 2010), in particular para 28. See also Article 29 Working Party, Statement on the role of a risk-based approach in data protection legal frameworks (WP281, 30 May 2014), para 6, which makes a distinction between transparency and accountability.

[13] Office of the Privacy Commissioner of Canada, Interpretation Bulletin: Accountability, https://www.priv.gc.ca/leg_c/interpretations_02_acc_e.asp.

[14] *Nammo v. Transunion of Canada Inc*., 2010 FC 1284; *Landry v. Royal Bank of Canada,* 2011 FC 687.

[15] See Thomas N Hale, 'Transparency, Accountability, and Global Governance' (2008) 14 Global Governance 73.

Directive effectively stalled the widespread adoption of electronic signatures by limiting market demand for technology innovations which fell outside the law's prescriptions.[16]

Guidelines and recommendations also need to avoid this danger of being over prescriptive. For this reason we have adopted a layered model here, similar to that used for analysing the concept of accountability. The highest layer is a general description of what a cloud contract ought to contain on this topic. Subsequent layers are increasingly granular and more focused on particular activities. The language used is behaviour-shaping ('should' or 'ought) rather than imperative ('shall' or 'must'). At the lowest level we have included some recommendations relating to privacy, both to make clear the links with the A4Cloud work in this area and to highlight issues which the OECD might wish to consider.

A further issue which is worth mentioning is the analytical organisation of this section. Because the focus of this deliverable is on accountability, we have arranged our analysis under each of the five accountability attributes. This is a theoretical, rather than a practical, arrangement, and if UNCITRAL and the OECD make use of this work, their own guidelines and recommendations are more likely to be organised in functional terms, for example under headings such as 'data security'.

3.1 Transparency

As previously stated, transparency is often seen as the most important of the Accountability Attributes. Previous research by A4Cloud's legal and regulatory team has highlighted many of the areas where transparency is currently lacking[17], and work on the COAT tool[18] has identified the core pre-contractual information which is needed to make a choice of cloud service provider.

The basic principle of transparency can be formulated as follows:

- A cloud provider should, voluntarily and where possible in advance, make available to potential and existing cloud customers all the information which the provider might reasonably expect a customer to be entitled to in order to:
  - make an informed decision whether to use that cloud providers services
  - use the provider's services effectively in conjunction with their own systems and third-party systems and services
  - comply with legal and regulatory obligations

  Commentary: At first sight it seems obvious that the provider should simply make available all the information which its potential customers might want. However, further thought reveals an important constraint, that there is necessarily a trade-off between the customer's desire for the utmost transparency and the provider's need to maintain some information as confidential. This might be for reasons of commercial secrecy (e.g. disclosing a list of sub-providers might expose proprietary elements of the provider's business model) or because of the provider's national security obligations (e.g. national law might forbid disclosing law enforcement requests for data access). A reasonable cloud provider would, though, investigate alternative means of

[16] Report from the Commission to the European Parliament and the Council on the operation of Directive 1999/93/EC on a Community framework for electronic signatures, COM(2006) 120 final 15 March 2006, 5-8. See further Chris Reed, *Making Laws for Cyberspace* (Oxford: OUP 2012) Ch 8.

[17] Niamh Gleeson (ed), *Survey of cloud standard contract terms and SLAs in 2015* (2015 FP7 A4Cloud project deliverable D-4.2).

[18] Dimitra Stefanatou (ed), *Guidelines and tools for cloud contracts* (2015 FP7 A4Cloud deliverable D-4.3, currently under review by the European Commission).

providing the assurance to customers which direct access to information would give, such as by commissioning audits by trustworthy persons and disclosing the audit findings.

Each of these sub elements can then be expanded to give example lists of the kinds of information which a cloud provider might be expected to make available. Thus, as an example:

- In order to make an informed decision about whether to use a cloud provider's services, the cloud customer might need, inter alia, the following information:
  - corporate and financial information about the cloud provider
  - a comprehensive description of the services and their service levels
  - any technical standards with which the services comply
  - access to the terms of service, privacy policy, acceptable use policy, and any other similar documents
  - the geographical location or residence of the entity providing the services and any regulatory regime to which that entity and/or the cloud provider is subject
  - the geographical location or locations where data will or might be processed
  - the extent to which sub-providers are used in the provision of the services[19]
  - access by the customer to data once the services relationship has ended, and post termination storage and deletion of that data
  - in what circumstances, and under what safeguards, the provider will permit third parties access to the customer's data and applications

Commentary: This list is not intended to be comprehensive, but represents those matters which the A4Cloud review of provider contractual documents[20] has discovered are commonly not fully disclosed or explained. Two elements of the list are potentially controversial: disclosure of sub-provision, both because this can disclose commercial secrets of the provider and because the cadre of sub-providers may be dynamic, constantly changing in membership and function; and the provision about third party access, which is complicated by the provider's need to comply with national law requirements which may be complex and hard to apply outside the specific context of a third party demand for access.[21] However, the aim of this list is not to be prescriptive, but rather to indicate the kinds of matters which an accountable provider would need to consider for transparency. An accountable provider should also seek ways to provide assurance to customers where it is inappropriate or unlawful to disclose detailed information; as an example, in the case of sub-providers the provider might be able to explain in general terms the roles

[19]We have intentionally used open-textured language here to allow for a range of differing national approaches. For example, the Article 29 Working Party further recommends in this respect that 'There should be a clear obligation of the cloud provider to name all the subcontractors commissioned.', Opinion 05/2012 on Cloud Computing. However, this approach will not find favour universally, and recommending at too detailed a level is likely to be an obstacle to progress on guidelines at an international level.

[20] n 17.

[21] See eg the ongoing litigation in *Memorandum and Order, In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp* (SDNY Apr 25, 2014), currently under appeal, in which the US Department of Justice has demanded access to an email account hosted by Microsoft's Irish subsidiary .

undertaken by sub-providers and how relevant attributes, such as their trustworthiness, were assessed.

An important aspect of the transparency which customers need in order to comply with their legal and regulatory obligations is information relating to data protection and privacy compliance.

- A cloud provider should, voluntarily and where possible in advance, make available to cloud customers all the information which the provider might reasonably expect a customer to be entitled to in order to be satisfied that personal data will be processed appropriately and that the customer can account to a cloud subject for that processing

Further elaboration is then appropriate, focusing on the kinds and level of information which would meet that guideline:

- When making privacy-related information available to cloud customers a cloud provider should ensure that:
    - Privacy policies are written in an language which is understandable by non-experts
    - Privacy policies are sufficiently detailed to enable the customer to understand the privacy implications of the service
    - Cloud customers are kept informed about changes in privacy policies, and in particular:
        - Given reasonable advance notice of changes;
        - Changes are summarised in an accessible manner; and
        - Changes are not made with excessive frequency.
    - Complaint forms avoid legal and technical terms and are usable by non-experts
    - There are clear contact points for queries in relation to the personal information entrusted to the service
    - So far as is reasonable the provider discloses:
        - the geographical location or residence of the entity providing the services and any regulatory regime to which that entity and/or the cloud provider is subject
        - the geographical location or locations where data will or might be processed
        - any use of sub-providers and the role they play in the context of processing[22]

Commentary: The first two elements here are, of course, conflicting because it is notorious that internet users, including business users, will not read documents of any length. Layering of privacy policies is one potential solution, though it creates the risk that important information may

[22] See discussion in n 19 on the language used here.

be omitted from the highest layers and thus never be read.[23] The potential difficulties involved in disclosing geographical locations and sub-provision have already been explained above.

3.2 Responsiveness

Recommendations and guidelines about responsiveness will necessarily be far less detailed than for transparency, because the provider is accepting an obligation to respond to specific requests. There are two main aspects to responsiveness: responding to requests for information, and responding to requests to take action in respect of customer data.

- A cloud provider should respond to all reasonable requests from a potential or existing cloud customer[24] for:
    - Information which the customer requires in order to decide whether to use the provider's services
    - Information about how the customer's data is being processed by a provider or sub-provider, either in general or in relation to specific data
    - Information about disclosure of the customer's data to third parties

Commentary: As is the case for transparency, 'reasonableness' is intended to indicate a balance between the customer's needs and those of the provider. What is reasonable will depend very much on context, including the nature of the service. For example, if the service is a low-price/mass-market service, then the cost of responding to individual requests might be entirely out of proportion to the potential revenue from each customer, in which case it might be reasonable not to respond at all.

- In relation to its processing of data, a cloud provider should respond to all reasonable requests from a cloud customer for:
    - Access to or copies of the customer's data
    - Deletion of the customer's data
    - Blocking of future actions in respect of specific customer data

Commentary: Even where a service is comparatively highly priced, the cost of responding to requests of this type is likely to eat substantially into the provider's margins, and thus seems unreasonable from the provider's perspective. This is where automated tools, such as those being developed by A4Cloud, can play an important part, effectively giving the customer direct access to the required information without incurring further cost to the provider.

---

[23] See Dimitra Karaminou, Christopher Millard and W Kuan Hon, Privacy in the Clouds: An Empirical Study of the Terms of Service and Privacy Policies of 20 Cloud Service Providers (Queen Mary School of Law Legal Studies Research Paper No. 209/2015, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2646447) 13.

[24] Because the focus here is on the contract between provider and customer, it does not deal with information requested by cloud subjects (eg data protection access requests, information about transactions between the subject and the customer, etc). However, if the customer wishes or is obliged to give that information to cloud subjects, it will be information which it is reasonable for the customer to request from the provider, and thus fall within this recommendation.

Additional responsiveness elements will be required to deal with the customer's obligations to those whose personal data it processes and to its privacy/data protection regulatory authority:

- Cloud providers should be appropriately willing to provide access to information and systems which is needed by cloud customers to comply with their obligations to regulators, and to co-operate with those regulators

Commentary: A4Cloud has identified and analysed the growing trend for privacy/data protection regulatory authorities to deal with data controllers by means of investigations and audits, rather than simply by responding to complaints from data subjects.[25] Such investigations can extend to examination of data processing transactions at the level of individual records, and so where the data controller is a cloud customer, the customer will require assistance and co-operation from its provider in order to satisfy the regulatory authority.

3.3 Responsibility

In this discussion it is important not to confuse responsibility with liability (which is dealt with under remediability in the next section). Responsibility on the part of a provider means that the provider accepts that it has an obligation to perform a particular function, and conversely makes clear when it has no such obligation. A simple example might be backing up of data: for some services the provider will make backups and restore data from them in the case of problems; for other services, the customer might need to make its own backup arrangements. Either might be the optimum solution in a particular context, but the worst possible position is where neither has clear responsibility for the backup function. In general the law requires factual responsibility as a prerequisite to liability, but not always – it is not uncommon for 'strict' no-fault liability to be imposed by law, or even liability for acts for which another person is factually responsible. Conversely, factual responsibility might exist in the absence of liability (for example, the intermediary immunities discussed in Appendix 2.3) or a provider might successfully exclude legal liability for matters for which it is factually responsible.

At the current stage of cloud development, providers are still uncertain what responsibilities they can safely undertake[26] without threatening the continuance of their business activities, precisely because although responsibility is not the same thing as liability, accepting responsibility creates liability risks.[27] It is therefore too early for recommendations/guidelines to attempt to prescribe a list of responsibilities.

Instead, the focus should be on persuading providers to undertake a wider range of service obligations, in particular those obligations which assist customers to achieve compliance. Failure to achieve a service obligation at the service level specified is objectively assessable, and is normally compensated only by service credits, which are a reduction of the service fee. These two elements help to reduce the liability risk of accepting responsibility to a manageable level.

---

[25] Asma Vranaki and Chris Reed, The Rise of Investigations by European Data Protection Authorities in the Context of Cloud Computing" (2015, FP7 A4Cloud project deliverable D-4.11); Asma Vranaki and Chris Reed, "The Role of Law in Regulating the Investigations of Cloud Providers by EU DPAs" (2015, FP7 A4Cloud project deliverable D-4.4); Asma Vranaki and Chris Reed, "Cloud Investigations by European Data Protection Authorities: An Empirical View" (2015, FP7 A4Cloud project deliverable D-44.11(2)).

[26] Deliverable D-4.2, n 17.

[27] Though, in spite of what some providers appear to think, denying responsibility does not of itself prevent legal liability arising, eg in the case of consumers who will benefit from responsibility terms implied at law, such as that under the UK Supply of Goods and Services Act 1982, s 13, that the provider will exercise reasonable care and skill in supplying the services.

Thus the basic responsibility guideline could be expressed as follows:

- Cloud providers should:
  - set out the service obligations which they commit to meet and the level of service to which they commit for each obligation
  - explain clearly to customers the allocation of responsibility between themselves and their sub-providers for any data handling which is not covered by a service obligation
  - explain clearly to customers the data handling matters for which the customer is responsible, including any tools provided by or recommended by the provider to assist the customer

There is, as yet, no clear consensus on how to categorise the service obligations which a cloud provider should at least consider accepting, but at a high level the following list is likely to achieve some consensus, at least as an aspirational target:

- The service obligations to which a cloud provider might commit include, inter alia, obligations relating to:
  - service availability
  - response time
  - query handling
  - data access and portability
  - data deletion
  - data security and physical security
  - security and data breach incident management
  - backup and restore

Commentary: These obligations are a subset of those suggested by the Cloud Select Industry Group's *Cloud Service Level Agreements Standardisation Guidelines*.[28] At present, in most mass-market cloud computing contracts service availability is the only service obligation to which cloud providers commit, but there are signs that providers may gradually undertake more extensive service obligations as they become more comfortable that they can assess and manage the risks such obligations create.[29]

3.4 Remediability

Remediability means that, having accepted responsibility for a failure, the cloud provider also undertakes to provide some remedy to the customer. It is important to stress here that a remedy need not always take the form of financial compensation – in many cases it will be entirely satisfactory if the failure is remedied, eg where wrongly deleted data is restored. There will also be many failures where

[28] https://ec.europa.eu/digital-agenda/en/news/cloud-service-level-agreement-standardisation-guidelines
[29] Deliverable D-4.2, n 17, 4.5.

self-help remediation can be achieved by use of technical tools, made available by the provider for use by the customer, and these tools are an important focus of the A4Cloud research.

Where financial compensation is the only feasible remedy, the liability problem surfaces. Liability is a very real problem because a cloud provider is a point of concentration for claims which have the potential vastly to exceed a service's annual revenue in respect of a single breach. For this reason, providers normally exclude all financial liability except in negotiated relationships with substantial customers.[30] However, the service obligation/level/credit regime, discussed in the previous section, has the potential to provide at least some financial compensation without raising this concentration risk, and we therefore think that guidelines/recommendations should focus strongly on that.

At the highest level:

- Cloud providers should offer appropriate remedies to their customers for service failures, and in particular:
  - Service level agreements should offer a ladder of remedies for poor service automatically, without the need for a customer to make a claim, eg via service credits
  - Appropriate remediation measures should operate along the cloud supply chain
  - The applicable law and jurisdiction for liability claims should be clearly stated and such statements of applicable law and jurisdiction should be accurate in the light of mandatory national law provisions
  - Limitations on liability should be clearly stated, and should take account of the special position of customers who act as consumers
  - Acceptance of liability by providers should be appropriate in the light of insurance availability

  Commentary: Applicable law and jurisdiction is an area of law where uncertainty abounds, but it can be reduced if cloud contracts make clear provision. Because such contracts are often cross-border, though, it will be common for the chosen law and jurisdiction to be foreign, so far as the customer is concerned, and this can act as a deterrent to claiming remediation. Because national mandatory laws can often upset choice of law and jurisdiction clauses, it would be ideal if the provider took these into account so that the contractual statements were truly accurate. Similar reasoning applies to consumer claims, because liability limitations are often unenforceable against consumers.[31]

Although the liability problem means that detailed guidelines on remediation are unlikely to achieve widespread acceptance at this stage, some high level guidelines might be acceptable:

- Cloud providers should:
  - provide an appropriate remedy to customers for failure to achieve service levels
  - explain clearly to customers the extent to which they accept liability for losses suffered by the customer (other than failure to achieve a service level)

[30] Ibid, 3.13-3.17.
[31] Eg under Directive 93/13/EEC on unfair terms in consumer contracts, OJ L 95 April 21 1993.

- explain clearly to customers the non-financial remedies which the provider is prepared to offer

- explain clearly to customers any steps the customer can itself take to remedy issues, including any tools made available by or recommended by the provider[32]

These last two bullet points are particularly relevant to service failures which potentially have a data protection or privacy impact. An accountable cloud provider should, in order to provide remediability, devise a range of measures to reduce the impact of any service failures which threaten the privacy of personal data. In terms of remediation, there should be contractual promises to do so:

- So far as is practicable, cloud providers should commit contractually to making tools and other mechanisms available to cloud customers to assist those customers in remedying the consequences of any service failures. Mechanisms might include:

  - devising incident management programs appropriate to the type of personal data processed

  - remedying failures which threaten the privacy of personal data, and reducing the impact on privacy of such failures

  - ensuring that appropriate remediation measures operate along the cloud supply chain

  - allocating responsibility to specific departments and named contact points for incident handling in their privacy management programs

  Commentary: Self-help remediation via tools and mechanisms is an important focus of the A4Cloud research. The project's remediation tools[33] aim to demonstrate how giving customers direct access to remediation facilities, for example allowing customers to delete data directly and prevent further loss, can often provide a more effective remedy than retrospective compensation after the event. Among the advantages of such tools are that they allow the customer to control the remediation process, and thus enhance confidence that remediation has occurred effectively, and that they can provide quicker action in response to a failure, eg if the failure affects such a large number of customers that the provider will inevitably require time to deal with all the consequences.

3.5 Verifiability

Verifiability is achieved by a cloud provider producing evidence about both service failures *and* the proper functioning of the service. Service failure is normally exceptional, but it is common for apparently proper functioning to be taken at face value without inquiry as to whether in fact it is occurring. By the nature of cloud computing, many instances of improper functioning will be invisible to customers, such as data storage outside the agreed geographical location(s). Thus an accountable provider will be able to give reassurance on this issue, through system logs, audits, periodic reports, etc. This evidence will also help identify and explain the reasons for any service failures.

[32] Note that the Redress & Remediation Tool developed by the A4Cloud Project attempts to demonstrate how to implement this recommendation in practice, reflecting the conceptual model of accountability discussed in Section 2. The Redress and Remediation Tool, relevant for violations of the EU data protection law, will be discussed extensively under the A4 Cloud deliverable, 'D-4.4 Remediation guidelines and tools', due in December 2015.
[33] Ibid.

Verifiability is achieved through reporting mechanisms and technical tools, both of which must be operated by the provider. The production of tools to assist in verifiability is an important element of A4Cloud.

Guidelines and recommendations cannot be too specific about verifiability, because what evidence is providable and ought to be provided depends very much on the details of the service and that particular customer's needs. As a simple example, a customer in the financial services sector will need to provide a defined set of verifiability evidence to its financial regulator, whereas a customer who is a seller of goods has few regulatory obligations of this kind. Nonetheless, some recommendations are possible at a high level:

- A cloud provider should, so far as is reasonable, make available to its customers:
  - Evidence of the proper operation of its services
    - Sources of evidence might include internal investigations and audits, external audits and privacy/data protection investigations
  - Evidence of continuing adherence to standards and quality certification
  - Evidence that customer instructions have been carried out

Commentary: Providers who take verifiability seriously might even find some commercial advantages to doing so. Designing cloud systems and incorporating tools which produce verifiability evidence is likely to simplify and improve the provider's own internal management and audit processes. In addition, particularly where customers owe their own verifiability obligations to external stakeholders such as regulators, there may be a commercial opportunity in offering to those customers 'Compliance as a Service'.

Note that we suggest no recommendations about when a cloud customer should have a right to audit the cloud provider's systems. Audit is a complex issue which raises important data and systems security questions and is in any event a concept with a very variable meaning and potentially costly to implement. At the current state of development of cloud computing, audit rights can only be left to individual negotiation. However, the development of tools which will enable the customer to verify the workings of the provider's system in near-real time (such as A4Cloud's IMT tool) has the potential to lead to some levels of audit access being offered by providers, perhaps as part of their Compliance as a Service suite.

If UNCITRAL and the OECD were to include recommendations along these lines in any project relevant to cloud computing contracts, we suggest that an important first step to embedding accountability in the international legal framework would have been achieved.

4 Conclusions

We have previously commented on the range of understandings of the concept of accountability and the lack of any clear consensus about its meaning. The diversity of the documents we have referred to (see Bibliography) and which have relevance to, or make reference to, accountability confirms this lack of consensus.

In an attempt to bring some order into this chaos, we have focused on accountability as a core value, rather than merely as a mechanism to achieve some other end. Our aim has been to transfer attention from the organisational or technical ends to be achieved, such as controlling data location or preserving information security, to the behaviour of cloud service providers. If providers accept accountability as a core value which they ought to exhibit, they will inevitably wish to translate that value into their service

offerings. The result should be the achievement of the desired ends, but achieved in a way which fits with, and becomes an integral part of, the provider's business strategy.

It is, of course, difficult to translate a principle or a core value into actions. Section 3 of this deliverable attempts first steps to that end. Our hope is that international organisations such as UNCITRAL and the OECD will find our work sufficiently useful that it is worthwhile building it into their own projects.

Those who are committed to a particular view about how cloud providers should act, usually because their primary focus is on some sub-aspect of cloud computing such as data protection or data security, will inevitably find our approach both too unspecific and insufficiently prescriptive. This is, however, a deliberate choice on our part. Ever since the Internet became a tool for general use, the main experience of law and regulation in this arena has been of conflicting demands by lawmakers and regulators which are often wholly incompatible with each other. We believe that cloud computing, like any other global online activity, can only be regulated properly if these conflicting demands are reduced and eventually eliminated. The most likely way to achieve this end is to develop an international consensus at a high level, based on fundamental behaviour-shaping principles rather than on detailed prescriptions for behaviour.

However, we should stress that our focus on soft law in the form of recommendations and guidelines is intended merely as the start of the process, rather than an end in itself. Even if consensus is achieved at the high level we envisage, it will immediately become obvious that more detailed questions need to be answered. To give just two examples here:

- Cloud computing is a field in which there is a substantial power asymmetry between cloud providers and cloud customers. Cloud services are provided very much on a take it or leave it basis, with little scope for customers to negotiate differences.[34] Recommendations and guidelines aimed at cloud service providers might help rebalance some aspects of the power relationship, but it is unrealistic to expect cloud providers to act voluntarily in ways which contradict their fundamental commercial interests. National law will have a clear role to play here, partly through laws of general application such as competition or anti-trust law, and also through new laws which specifically address those imbalances which cannot be dealt with through soft law.

- Although international recommendations and guidelines would ideally accommodate the full range of national legal and cultural traditions, in practice some of these are so fundamentally incompatible that no accommodation can be reached. In the context of A4Cloud the most obvious of such incompatibilities is the conflict of approaches between the EU and the US on the question of privacy in personal data. The EU tradition requires a state-established supervisory authority, whilst the US tradition is wholly hostile to governmental involvement in regulating what are seen as essentially private relationships if state agencies are not undertaking the data processing. It might be that consensus can be reached on the fundamental principles of data protection[35], but choice of enforcement mechanisms will have to be left to individual states.

Nonetheless, we believe that working towards a soft law instrument covering cloud contracts, addressed to cloud providers and embedding accountability as a core value, is a worthwhile first step towards

[34]Hon W K, Millard C & Walden I, 'Negotiated Contracts for Cloud Services,' Ch 4 in Millard C (ed), *Cloud Computing Law* (Oxford University Press 2013). For a practical example, see Guido Noto La Diega & Ian Walden, *Contracting for the 'Internet of Things'. Looking into the Nest*, forthcoming.
[35] Using as a starting point GDPR art 5 (Commission text, n 36).

achieving an international system of law and regulation for cloud which offers the kind of consistency that all cloud actors, including lawmakers and regulators, require.

Appendices

1 Related legislative and soft law initiatives

1.1 Progress on the EU Legislative Framework

There are major developments currently ongoing at the EU level which are particularly relevant to accountability for cloud computing, in the areas of data protection and cyber security. In this Appendix we review the progress towards final resolution, noting that although the laws in question will have been enacted by early 2016, some of the issues are so fundamental that their final resolution is likely to take substantially longer.

The European Commission's original proposal for the GDPR[36] envisaged that it would be enacted by 2014 and come into force in 2016. However, the revised texts produced by the Parliament[37] and the Council[38] identified many areas of disagreement which have been referred to the negotiating process between the three institutions, the 'trilogue' process, which aims at producing an agreed text. The timetable for the trilogue began in June 2015, and the final meeting is scheduled for 15 December 2015. As the final editing of this Deliverable was completed it was announced that agreement had been reached and that the GDPR would be ratified by the EU institutions early in 2016.

However, a complication arises from the Court of Justice of the European Union (CJEU) decision in *Maximillian Schrems v Data Protection Commissioner*[39]. Here the court held that the Commission's decision[40] in 2000 to designate the US Safe Harbor scheme as providing adequate protection for exported personal data was invalid on a number of grounds. Perhaps the most important are that the decision did not appropriately investigate the safeguards provided by US law, particularly in relation to access to data by US law enforcement authorities[41], and that it made no provision for subject access, rectification or remedies, which are essential to maintain the protections for fundamental rights provided by EU law. As a consequence, the Safe Harbor in its current form will cease to operate (so far as EU data protection law is concerned) at the end of January 2016 as an exception to the data transfer rules in the DPD. If no solution is found, in the form of a new Safe Harbor agreement and decision, a number of EU data protection supervisors are prepared to commence enforcement action against companies transferring data to Safe Harbor subscribers.[42]

---

[36] Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data
COM(2012) 11 final.

[37] European Parliament legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)).

[38] Not publicly available, but the basis for political agreement on the way forward in June 2015: http://www.consilium.europa.eu/en/press/press-releases/2015/06/15-jha-data-protection/.

[39] Case C 362/14, 6 October 2015.

[40] Decision 2000/52, adopted by the Commission on the basis of Article 25(6) of Directive 95/46.

[41] The CJEU made specific reference to the Snowden revelations about the collection and monitoring of online communications by US authorities, in particular the National Security Agency, as revealed by the UK Guardian newspaper – 'NSA Prism program taps in to user data of Apple, Google and others', the *Guardian* 7 June 2013, http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data.

[42] Statement of the Article 29 Working Party, Brussels 16 October 2015.

The European Union's Commissioner for Justice, Consumers and Gender Equality, Commissioner Jourová in a speech on 15 November[43] predicted that agreement would be reached before the 31 January 2016 deadline, and this reflects the political imperative to produce an immediate solution. Of particular relevance to this deliverable, the Safe Harbor makes possible the activities of the major US cloud providers (and many other technology providers), so that failure to reach an agreement would be highly disruptive. However, any Commission decision re-validating the Safe Harbor would be likely to be challenged again before the CJEU, and informed insiders believe that it may be politically, and possibly even legally, impossible for the US to promise enough to satisfy the requirements of EU law even under the current Data Protection Directive.[44] The additional protections which the GDPR[45] is likely to introduce will make reaching a final agreement which survives legal challenge even more difficult, as will those incorporated in the proposed Directive on data protection and law enforcement[46], given that they touch upon fundamental aspects of EU data protection law (eg allocation of new obligations on controllers, role of national supervisory authorities) which affect law enforcement and national security. These are matters that each nation state considers to be fundamental issues about which it alone should make decisions. A further difficulty is that there is a fundamental conflict between the imposition of EU law extraterritorially on foreign-established actors such as cloud providers; in the US this might conflict with the 'due process' clause of the US Constitution[47], a matter which is reserved to the courts to decide and can therefore not be dealt with by negotiation with the US Government.

As far as the area of cybersecurity is concerned, on 7 December 2015 the EU lawmakers and Member States reached an agreement on the first cybersecurity law applicable across different industry sectors. According to the European Commission Vice-President for the Digital Single Market, Andrus Ansip, the new law would strengthen consumers' trust in online services, especially, cross-border services, adding further in this respect that 'The Internet knows no border - a problem in one country can have a knock-on effect in the rest of Europe. This is why we need EU-wide cybersecurity solutions.'[48] The agreement on the adoption of a cybersecurity Directive within the EU follows from an earlier initiative taken by the European Commission to release a "*Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*[49]" ("the Cybersecurity Strategy") along with a proposal for a Network and Information Security (NIS) Directive.[50] The Directive is a minimum harmonisation[51] one, which aims at ensuring a higher level of data security across the whole EU by setting a threshold that national laws must meet, while still having the possibility to exceed the minimum mandatory level. This proposal represented at the time the EU's first attempt to enact a comprehensive set of cyber security related norms that are not restricted to a particular area or regulatory sector. The recent agreement on the

[43] http://fedscoop.com/european-commissioner-well-have-new-safe-harbor-deal-before-deadline

[44] Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L281/31, 23 November 1995.

[45] Hon, W. Kuan and Kosta, Eleni and Millard, Christopher and Stefanatou, Dimitra, Cloud Accountability: The Likely Impact of the Proposed EU Data Protection Regulation. Queen Mary School of Law Legal Studies Research Paper No. 172/2014; Tilburg Law School Research Paper No. 07/2014. Available at SSRN: http://ssrn.com/abstract=2405971 or http://dx.doi.org/10.2139/ssrn.2405971

[46] Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties and the free movement of such data (COM(2012)10 final, 27 January 2012, original text; 12266/15, 2 October 2015, revised text).

[47] The Fifth and potentially also the Fourteenth Amendments to the US Constitution.

[48] "EU lawmakers, countries agree on cyber security law", available at http://www.euractiv.com/sections/digital/eu-lawmakers-countries-agree-cybersecurity-law-320212

[49] European Commission, joint communication to the European Parliament, the council, the European Economic and Social Committee and the Committee of the Regions, "*Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*", JOIN (2013) 1 final, Brussels, 7.2.2013.

[50] European Commission, "*Proposal for a Directive Of The European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union*", COM (2013) 48 final, 2013/0027 (COD), Brussels, 7.2.2013.

[51] See Art. 2, Commission's proposal for a NIS Directive. See also European Commission, "*Proposed Directive on Network and Information Security – frequently asked questions*", Memo, Brussels, 7.2.2013.

adoption of a Directive, which is also likely to achieve formal approval in early 2016, forms a major shift towards a mandatory scheme for cooperation and incident notification across Member States.[52]

1.2 Other Cloud Relevant Initiatives

The EU regulation on personal data breaches[53] requires public electronic communications providers such as telcos and ISPs to report such breaches to the relevant national regulator, and this has led to a range of national guidance on when and how such reporting should be made.[54] ENISA has also produced extensive guidelines on this matter.[55]

Sector-specific guidance on personal data breach has also been produced, such as the IG Toolkit Incident Reporting Tool[56], use of which is mandatory in the UK healthcare sector, and the Italian decisions relating to the banking[57] and biometric data[58] sectors.

Outside the field of personal data breaches, there is also a range of guidance and recommendations specifically aimed at cloud computing. The Australian Government's Cloud Computing Policy usefully summarises the extensive guidance which the Australian authorities have produced on a range of issues in cloud computing, many of which have relevance for accountability.[59] In other countries, cloud data security[60] and cloud privacy/data protection[61] have received specific attention.

All these initiatives aim to impose obligations on cloud actors to act in particular ways. The principle of accountability requires those actors to give an account of how far they have met their obligations, and so these initiatives give some idea as to the necessary content of any account. Data breach initiatives

---

[52] Note that the cyber-security Directive will be further discussed under "D-4.4 Remediation guidelines and tools", due in December 2015.

[53] Commission Regulation (EC) 611/2013 of 24 June 2013 on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC of the European Parliament and of the Council on privacy and electronic communications [2013] OJ L173/2.

[54] See eg UK ICO, Notification of data security breaches to the Information Commissioner's Office (2012), https://ico.org.uk/media/for-organisations/documents/1536/breach_reporting.pdf; Belgian Commission de la protection de la vie privée, Recommandation n° 01/2013 du 21 janvier 2013, https://www.privacycommission.be/sites/privacycommission/files/documents/recommandation_01_2013_0.pdf.

[55] Andreas Rockelmann, Joshua Budd, Michael Vorisek, 'Data Breach Notification in the EU' (ENISA, 13 January 2011); Marnix Dekker and Christoffer Karsberg 'Technical guidance on the incident reporting in Article 13a' (ENISA, November 2013); Marnix Dekker, Christoffer Karsberg 'Technical guidance on the security measures in Article 13a' (ENISA, November 2013).

[56] https://www.igt.hscic.gov.uk/resources/IG%20Incident%20Reporting%20Tool%20User%20Guide.pdf.

[57] Data Sharing and Tracking of Transactions in the Banking Sector, Decision by the Italian DPA of 12 May 2011 as published in Italy's Official Journal no. 127 dated 3 June 2011, http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1868766.

[58] Rettifica alla Deliberazione n. 513 del 12 novembre 2014 recante 'Provvedimento generale prescrittivo in tema di biometria' - 15 gennaio 2015 (Pubblicato sulla Gazzetta Ufficiale n. 34 dell'11 febbraio 2015), http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3556992.

[59] Australian Government Cloud Computing Policy (2013) 11-4, http://www.finance.gov.au/files/2012/04/Australian-Government-Cloud-Computing-Policy-Version-2.0.pdf

[60] See eg Marnix Dekker, Dimitra Liveri, Matina Lakka, 'Cloud Security Incident Reporting - Framework for reporting about major cloud security incidents' (ENISA, 9 December 2013); UK ICO, Guidance on data security breach management (2012), https://ico.org.uk/media/for-organisations/documents/1562/guidance_on_data_security_breach_management.pdf; CSI-SLA Subgroup (European Commission), *"Cloud Service Level Agreement Standardisation Guidelines"*, 2014, https://ec.europa.eu/digital-agenda/en/news/cloud-service-level-agreement-standardisation-guidelines.

[61] CNIL, "Recommendations for companies planning to use Cloud computing services", available at http://www.cnil.fr/fileadmin/documents/en/Recommendations_for_companies_planning_to_use_Cloud_computing_services.pdf; Article 29 Working Party, "Opinion 02/2015 on C-SIG Code of Conduct on Cloud Computing" (WP232), adopted on the 22nd of September 2015, available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2015/wp232_en.pdf

are particularly interesting, because they usually contain specific obligations to notify data subjects, and in some cases data protection or privacy regulators and others, that the breach has occurred and what steps are being taken to remedy it. Such a notification is a form of account, but will not necessarily comply with the A4Cloud conception because, as is the case for all these initiatives, their focus is universally activity- or sector-specific. They begin by identifying the mischief to be guarded against, for example data breaches, and then prescribe the actions to be taken if the mischief occurs. The required actions might include providing an account, but the account will be focused firmly on the specific mischief in question. In contrast, this Deliverable has taken accountability as its starting point, as an overriding value, and attempted to show in Section 3 how it might be embedded at a transborder level so as to guide and shape future regulatory initiatives.

2 A Road Map for Embedding Accountability

2.1 The Road Map

Although this Deliverable is concerned only with legal and regulatory issues, it is important to note that law and regulation is not the sole, nor even the primary, route to achieving accountability. Industry initiatives, standards setting, research findings and market pressure are far quicker ways of embedding accountability in the practice of the cloud computing sector. However, law and regulation provide the back-stop which deters and sanctions free riders who decide not to be accountable. If, as we assert, accountability is a fundamental value for cloud computing, then it is important for this value to be embedded in law and regulation globally.[62] This Appendix therefore examines how international initiatives to produce a globally consistent legal framework proceed.

The ultimate end point of an initiative to generate legal and regulatory consensus at an international level is full approximation of national laws by means of a formal, binding international instrument such as a Convention, potentially embedding legal principles, as for instance, accountability. Such an instrument obliges signatory states to amend their national laws so as to comply with the Convention, and thus results in a functionally equivalent legal framework across all signatory states. Of course, not all initiatives reach this end point – in many cases, once international consensus is reached on the basic principles which are to be incorporated, a suitably uniform global legal framework can be achieved by adopting different means in different states. This is particularly likely if national differences of approach can be accommodated through contractual provisions, and is an important reason why Section 3 focuses on recommendations and guidelines for cloud contracts.

The usual means by which international discussion progresses towards international consensus on law is as follows.

The first stage is that one or more authoritative international bodies accepts that there is a need for global action to approximate national laws, and issues guidelines and/or recommendations. These might address national lawmakers, who will take them into account when framing new laws in the field, or could be addressed to those who are operating in the field so that contracts and business practices can be influenced. There are two international bodies which have previously undertaken such work on the legal issues arising from transnational data processing activities: UNCITRAL, the UN Commission on International Trade Law in relation to e-commerce and e-signatures; and the Organisation for Economic Co-operation and Development (OECD) in relation to data privacy. These guidelines and recommendations have proved influential in shaping national laws.

The second stage is the recursive process of revising guidelines and recommendations in the light of experience of national law solutions and changes in technology and business practice. This stage is important because it identifies unanticipated difficulties in the original text, usually based on input from those who are trying to implement the guidelines and recommendations. Revised versions can be produced comparatively easily, and at some point there might be sufficient consensus that a solution has been reached for these to become definitive – in the case of UNCITRAL, the process often results in a Model Law which can be adopted, in whole or in part, by national lawmakers.

The third and final stage, once international consensus has been achieved, is to assess the need for, and feasibility of achieving, a formal legal instrument. The work of OECD on data privacy has so far only

[62] It might be objected that the fundamental differences between states, particularly on human rights issues, are so great that there is no point even in making a start. Our response would be that there is already a high level of consensus about these fundamental values, at least between the states where major cloud providers are established. These are the states which might consider implementing the initiatives we propose. Most of the disagreements lie in the area of implementation, some of which are discussed below in Appendix 2.3.

resulted in guidelines, mainly because there are still substantial national differences in the approach to issues of data privacy. In the field of e-commerce UNCITRAL has issued Model Laws which have been very influential on national law development. A formally binding instrument is distinctly a long-term prospect for most aspects of computing technology, but an example of achieving such an instrument is the Council of Europe's Convention on Cybercrime[63], which deals with urgent matters of public security and is evolving into a fully transnational legal instrument as more and more signatories outside Europe adopt the Convention.

Because we are currently at the very beginning of the process we have described, in the sense that it is only now that international bodies have begun acknowledge the need to take action and regulate the cloud industry at a global scale, the focus of this deliverable is on 'soft' law mechanisms (guidance, models, recommendations), or in other word, stage 1 of the process described above.

2.2 Scope

There are two areas where guidelines/recommendations would be appropriate to begin the process of embedding accountability into the international legal framework.

The first would be guidelines or recommendations relating to cloud contracts, most appropriately produced by UNCITRAL. The work of UNCITRAL focuses on international trade law, and cloud computing is an important new trade activity which falls clearly within its remit. UNCITRAL is considering a project in this area and has asked QMUL's Cloud Legal team for initial comments, to which the A4Cloud legal and regulatory team contributed. Those parts of this deliverable which relate to UNCITRAL's work are an expansion of those comments, and are aimed at assisting UNCITRAL to take the project forward. This work would, of course, take into account the existing work of government agencies and private sector bodies, which has already identified many of the issues which would need to be considered and dealt with.[64]

These guidelines or recommendations would be aimed at:

- Assisting the cloud customer to select cloud services which are appropriate for the customer's needs and which will enable the customer to comply with law and regulation;
- Increasing the availability of information about cloud services which relates to customer compliance;
- Increasing service provider transparency about incident handling (eg. data breaches);
- Enhancing service provider adherence to best practice;
- Persuading service providers to give greater assurance that they are providing the services in accordance with their description (which would include the compliance information above).

[63] http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.

[64] See in particular the sources discussed in Section 1.2, together with the Cloud Industry Forum's Code of Practice (http://www.cloudindustryforum.org/content/code-practice-cloud-service-providers) and the Cloud Security Alliance's Security Guidance (https://cloudsecurityalliance.org/group/security-guidance/). The work of governmental agencies on cloud procurement is also useful in this respect – see eg US Chief Acquisition Officers Council, *Creating Effective Cloud Computing Contracts for the Federal Government* (2012, https://cio.gov/wp-content/uploads/downloads/2012/09/cloudbestpractices.pdf).

The intended effect of such measures should be to embed accountability to customers as a potential market advantage for service providers, by providing a benchmark against which they can be compared with other providers[65].

The second is in relation to privacy, an area in which the OECD has already produced guidelines on the wider issues of digital privacy. As early as 1980 the OECD published a Recommendation providing, specifically, for 'the protection of privacy and the transborder flows of personal data'[66]. Article 14 of the Guidelines introduces accountability as a separate fundamental privacy principle dictating that: 'A data controller[67] should be accountable for measures which give effect to the principles stated above'. By embedding accountability in text, the OECD aimed to ensure the effectiveness of the rest of the principles provided (ie. openness, use limitation, purpose specification)'. Accountability also aims at ensuring that personal information will be adequately protected regardless of the location where it will be processed, by holding data controllers to account for the enforcement of the fundamental privacy principles introduced. In this respect, it has therefore been argued that the OECD Guidelines should 'make it clear that an organisation should retain responsibility for privacy regardless of where the data resides and to whom it has been transferred or disclosed'[68].

The 1980 Guidelines were revised in 2013 and introduce an entirely new part setting out how organisations could implement accountability in concrete terms. Article 15 of the text dictates that data controllers should be assigned with the obligations to: a) to put in place privacy management programs meeting specific requirements (eg scalability), b) 'to be prepared to demonstrate its privacy management program as appropriate' and c) to provide notice in case of security breach of personal data[69]. Note that the Guidelines emphasise the need for data controllers to demonstrate how their privacy programs achieve compliance with codes of conduct or any other legal mechanisms giving effect to the Guidelines. Overall, the new part of the OECD revised Guidelines regulating accountability is considered to be the "only significant positive addition'[70].

---

[65] Note that the A4Cloud Project has created a Cloud Offerings Advisory Tool (COAT), which aims at assisting cloud customers in selecting a cloud service provider from a list of proposed providers that would best correspond to their business needs and preferences. For more on the identified areas considered within the project research meaningful to compare for accountability purposes, see Dimitra Stefanatou (ed), *Guidelines and tools for cloud contracts* (2015 FP7 A4Cloud deliverable D-4.3, currently under review by the European Commission). The analysis in that document of the factors in respect of which cloud customers ought to have transparency should be fed into the development of UNCITRAL's recommendations, once high level agreement on the principles set out in this Section have been agreed.

[66] Organisation for Economic Co-operation and Development (OECD), Recommendation of the Council concerning Guidelines governing the protection of privacy and transborder flows of personal data, 23 September 1980, available at: http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

[67] For the purposes of the OECD Guidelines, *'data controller' means a party who, according to domestic law, is competent to decide about the contents and use of personal data regardless of whether or not such data are collected, stored, processed or disseminated by that party or by an agent on its behalf*;

[68] 'Getting to Accountability, Maximising your Privacy Management Program. A privacy officer's guide to achieving the highest level of accountability possible based on available resources Version 3.0 - 19 August 2015, page 5, available at https://www.nymity.com/data-privacy-resources/privacy-management-tools/~/media/NymityAura/Resources/Getting%20to%20Accountability/Nymity-Getting-to-Accountability-Paper.pdf

[69] Organisation for Economic Co-operation and Development (OECD), Recommendation of the Council concerning Guidelines governing the protection of privacy and transborder flows of personal data, 11 July 2013, available at: http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf

[70] 'The Australian Privacy Foundation (APF), which represents privacy advocates, found the decision to leave the basic principles from 1980 unchanged to be a missed opportunity to respond to the developments of the last 35 years.' APF found the new part on implementing accountability to be the only significant positive addition', Robert Gellman: Fair Information Practices: A Basic History (November 13, 2015), available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2415020

> *Furthermore, the recently published OECD Recommendation on Digital Security Management[71], adds more on the role of accountability which is relevant for the domain of privacy. These Guidelines do not provide for accountability separately, but rather link it to the concept to responsibility and, in particular, to the ability to provide 'explanations about their actions or inactions (accountability)'[72]. In this context, accountability mandates that organisations justify in an open manner certain choices made leading further to actions or inactions[73]; organisations are, therefore, expected not only to give an account of what they did do or did not do, but also to explain why.*

If UNCITRAL and OECD decide to undertake work in this field there is a clear need for their activities to co-ordinate with each other. The terms of cloud computing contracts will, inter alia, set out what the provider promises to do in relation to data processing which affects privacy. Conversely, privacy obligations which are set out in any OECD guidelines will need to be reflected in the contracts between cloud customer and service provider, which would, therefore, emphasise in their clauses the role and the specificities of privacy programs. It would be unhelpful if the results of the two streams of work contained contradictory recommendations, or otherwise failed to achieve complementary results. This risk, which is always present when two organisations which have different memberships and working methods are operating in parallel, can be avoided by sharing documentation and seeking comments from each other.

For this reason we have included privacy-specific recommendations in the work on cloud contracts in Section 3, rather than dealing with them separately, so that they can be seen in their full context.

2.3 Foundational Principles

One-danger when producing recommendations or guidelines about a particular activity, such as cloud computing, is that those involved treat their work as a standalone activity. Cloud computing law is a sub-branch of technology law, and therefore needs to take into account the lessons which have been learnt in developing that law.

Technology-related law has come to recognise that there are a number of fundamental, or foundational, principles which are now widely accepted as being important to comply with when devising legal reforms. Compliance with these principles makes it more likely that the reforms will actually achieve their objectives, and assists in reducing conflict with other laws.

General Issues

The general issues are those which relate to all reform of laws which attempt to regulate information technology activities, and are thus not cloud-specific but nonetheless need to be considered and taken into account:

- T**echnology-neutrality.** At a high level, the principle that laws should be technologically neutral is widely espoused. In July 1997 the US Government published its *Framework for*

[71] OECD (2015), *Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document,* OECD Publishing, Paris. DOI: http://dx.doi.org/10.1787/9789264245471-en

[72] 'Stakeholders who decide to use the digital environment to achieve economic and social objectives (the drivers) are accepting a certain level of digital security risk – i.e. possible negative consequences. They should manage this risk, that is reduce it to an acceptable level on the basis of the four Operational Principles below. They should also be able to provide explanations about their actions or in actions (accountability).'

[73] Although privacy in personal data is often conceptualised in terms of active disclosure, many of the threats to privacy arise from simple inactivity. Examples might include failing to implement appropriate data security or failing to take action which might minimise the impact of a data breach.

Global Electronic Commerce, which stated that when regulating online activities, 'rules should be technology-neutral (ie, the rules should neither require nor assume a particular technology) and forward looking (ie, the rules should not hinder the use or development of technologies in the future)'.[74] The following year the term was used in EU legislative proposals for the first time[75] and has been adopted in relation to most EU technology legislation ever since.[76] Technology neutrality for online law has also been espoused extensively by national legislators and international organisations.[77]

If technology neutrality is achieved, laws exhibit a high degree of future-proofing. However, the concept of technology neutrality is quite complex, bearing a range of meanings and implementable in different ways with different consequences.[78] Thus lawmakers need to make sure they understand the concept fully and to apply it carefully, if its advantages are to be achieved.

Of course, cloud computing is a specific technology, so any law or regulation aimed at it would necessarily not be technologically neutral. However, this will in practice be dealt with when law and regulation defines the subject matter to which it applies, as 'cloud computing' is insufficiently precise for these purposes. A useful starting point might be the international standard ISO/IEC 17788:2014, which defines cloud computing as follows:

> *Paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand. NOTE – Examples of resources include servers, operating systems, networks, software, applications, and storage equipment").*

From a legal perspective, the most important elements appear to be: the provision of a data processing service; shared processing infrastructure; and that primary control over decisions about what data to process and how the results are to be used rests with the cloud customer rather than the provider.

- **Intermediary protections.** Similar to technology neutrality, there is also widespread international recognition that internet intermediaries, those whose primary activity is to carry, store and transmit data controlled by others, require special legal treatment. The application

[74] 1 July 1997 <http://www.technology.gov/digeconomy/framewrk.htm>.
[75] Opinion of the Economic and Social Committee on the 'Proposal for a Council Recommendation concerning the protection of minors and human dignity in audiovisual and information services', OJ C 214 10 July 1998, 25 para. 3.2.5: 'Regulation should be 'technology-neutral': as few as possible new regulations, policies and procedures should be specific to the new services.'; Recitals to the Proposal for a European Parliament and Council Directive on the taking up, the pursuit and the prudential supervision of the business of electronic money institutions, COM (1998) 0461 final, OJ C317, 15 October 1998, 7: '… this Directive introduces a technology-neutral legal framework that harmonises the prudential supervision of electronic money institutions to the extent necessary for ensuring their sound and prudent operation and their financial integrity in particular'.
[76] See eg Amended proposal for a European Parliament and Council Directive on a common framework for electronic signatures, COM (99) 195 final; Proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector, COM (2000) 0385 final, OJ C 365 E, 19 December 2000, 223; Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions - Electronic Communications: the Road to the Knowledge Economy, COM (2003) 65 final; Proposal for a Decision of the European Parliament and of the Council on establishing a multiannual Community programme on promoting safer use of the Internet and new online technologies, COM (2004) 91 final.
[77] Bert-Jaap Koops, 'Should ICT Regulation be Technology-Neutral' in Bert-Jaap Koops, Miriam Lips, Corien Prins & Maurice Schellekens, *Starting Points for ICT Regulation: deconstructing prevalent policy one-liners* (The Hague: TMC Asser Press 2006), 77, 77-9.
[78] See Chris Reed, *Making Laws for Cyberspace* (Oxford: OUP 2012) Ch 11.

of laws predating the internet age often resulted in decisions that those intermediaries were jointly liable with those who controlled data, even though the intermediary's only role was to store, carry or disseminate data on the instructions of the data's controller.[79] It was soon recognised that such joint liability might drive them out of business and thus lead to the collapse of the internet. A wide range of legislation introduced liability immunity for intermediaries who lacked knowledge of the content of the data they were processing, eg in the EU Directive on electronic commerce[80] arts 12-15 and the US Digital Millennium Copyright Act 1988 among others. The basic principle of this immunity is that it applies unless the intermediary receives notice of the unlawfulness of specific content and fails to act appropriately[81] in response to that notice.

Cloud providers and sub-providers share many of the characteristics of internet intermediaries, and so the principle of special treatment to avoid inappropriate imposition of joint liability should be adopted where possible for exactly the same reasons.

However, observance of this principle does not necessarily imply complete immunity from liability. The fundamental aim is to ensure that liabilities do not 'concentrate' on an intermediary to such an extent that it effectively becomes the insurer for those who should have primary responsibility for the liability-generating activity.

One way of observing the principle is to allow those involved to allocate liability between themselves, as in the Commission's Draft of Article 24 of the GDPR[82], which introduces a 'new obligation' regarding joint controllership:

> The Proposed Regulation contains a provision dealing with joint data controllers (Article 24), which requires them to conclude an 'arrangement' allocating data protection responsibility between them, which will require many companies to modify their commercial agreements.[83]

This provision will enable the joint data controllers to allocate responsibility, and thus liability, between them in a way which is more flexible and efficient than doing so in the substantive law.

- **Consumer protection.** Data privacy is of course deeply concerned with the interests of cloud subjects, but it is sometimes forgotten that cloud customers are often individuals whose interests are protected by consumer protection law. These laws differ widely in scope, but it is rare to find a country with no consumer protection laws at all. Thus work relating to cloud

[79] This class of internet intermediaries was the target of early litigation, and thus became the beneficiary of the immunities explained below. Many other types of online intermediary have since developed, such as trust service providers, payment providers, etc, but their activities do not expose them to the risk of liability for the actions of others. The class of search providers is controversial, with some limited immunities for search results in some countries – for an overview of the issues see James Grimmelmann, 'The Structure of Search Engine Law' (2007) 93 Iowa LR 1.

[80] Directive 2000/31/EC on electronic commerce OJ L 178/1, 17 July 2000.

[81] The most common action is to 'take down' the offending content, but the various legal instruments are complex on this point, because of the need to recognise that the person responsible for the content needs to be allowed to dispute its illegality.

[82] For more on the implications on cloud computing resulting from the Commission's proposal for a General Data Protection Regulation, see, also, D:B-5.1 White paper on the proposed data protection regulation, available at: http://www.a4cloud.eu/sites/default/files/D25.1%20White%20paper%20on%20new%20Data%20Protection%20Framework.pdf

[83] Christopher Kuner, 'The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law', BNA Bloomberg Privacy and Security Law Report (2012) February 6 2012, 1, 7.

contracts needs to recognise and deal with consumer issues so far as possible, leaving space for differences of national treatment.

There are also two issues of principle which relate only to the processing of data on behalf of another, but whose importance is increasingly being recognised:

- **Data and application interoperability and portability.** If cloud customers cannot move their data and applications between cloud providers they are effectively 'locked-in'. This means that market competition cannot work to drive increased accountability because customers are, for all practicable purposes, unable to take advantage of rival and more accountable offerings.

- **Data security.** Effective data security is a fundamental element of any computing service, and is important both for maintaining data privacy and also for the integrity of business operations. Data security is a moving target, and therefore unsuitable to be prescribed by law. However, accountability for data security is a mechanism through which improvements can be driven, and for this reason we think it required some mention in the Section 3 recommendations and guidelines.

Cloud-specific Issues

In cloud-specific terms we propose a further foundational principle, even though there is not as yet legal consensus at a transnational level on this matter. The principle is that the primary responsibility for achieving legal compliance in cloud computing in respect of how data is handled should be placed on the cloud customer, and that whether a similar responsibility should be imposed on the cloud provider is a matter to be left to national law and/or contracts between cloud provider and customer. These legal responsibilities would include privacy/data protection, compliance with third party contracts, and other regulatory compliance (eg in the financial sector).

Our reasons for proposing this principle are as follows:

- There is disagreement internationally about whether, if at all, cloud providers should have responsibility for their data processing to anyone other than cloud customers. The EU data protection regime represents perhaps one extreme of the continuum, with plans under the GDPR to extend some of the liabilities currently placed on cloud providers to their sub-processors as well. But even the EU regime recognises that most data protection obligations are primarily owed by data controllers, normally the cloud customer in this context, and so there is a consensus on this aspect of the issue.

- There is also no agreement about the shape of any cloud provider responsibility outside the provider/customer relationship. As an example, the EU data protection regime is predicated upon the existence of an external regulator to whom compliance duties are owed, whereas in the US (outside data processing by Federal and State bodies and in some specialist sectors) responsibility for privacy breaches is a private law matter between the parties.[84]

- The principle of intermediary special treatment, discussed at Appendix 2.3 above, would be respected by this approach, leaving it to national lawmakers to decide how far it was appropriate to override that principle in the light of their specific legal regime.

[84] For a helpful explanation of the reasons behind these differences see Andrew Charlesworth, 'Clash of the Data Titans? US and EU Data Privacy Regulation' (2000) 6 *European Public Law* 253. A recent explanation of the US data security regime is in Jared A Harshbarger,'Cloud Computing Providers and Data Security Law: Building Trust with United States Companies' (2011) 16 J Tech L & Policy 229.

- There is also a pragmatic advantage, that it makes identifying liability simpler, particularly in complex, cross-border incidents, and thus enhances the likelihood that the responsible person will take steps to provide redress.

Adopting this principle would, in our view, make it more likely that international consensus would be reached. In the longer term, the principle of accountability requires a cloud provider to account to a wider range of stakeholders than its customers, but an attempt to achieve this is likely to be too controversial at this stage, and might lead to the failure of the initiatives.

Applying the principle, the main role of the cloud provider (in terms of accountability) would thus be to assist the cloud customer to meet its own primary legal and regulatory obligations. This assistance would be offered by:

- Giving customers access to and use of data processing services;
- Providing information (to the customer at least, though the principles of accountability and of consumer protection suggests that some information should also be provided to the wider world) about how those services operate;
- Operating those services in accordance with the information provided to customers, and in accordance with good practice more generally.

Select Bibliography

This bibliography lists the most significant sources which are relevant to the discussion in this Deliverable.

Andreas Rockelmann, Joshua Budd, Michael Vorisek, 'Data Breach Notification in the EU' (ENISA, 13 January 2011)

APEC Privacy Framework, available at:http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx

Article 29 Working Party, Opinion 05/2012 on Cloud Computing

Article 29 Working Party, WP232 Opinion 02/2015 on C-SIG Code of Conduct on Cloud Computing.

Australian Government Cloud Computing Policy (2013), http://www.finance.gov.au/files/2012/04/Australian-Government-Cloud-Computing-Policy-Version-2.0.pdf

Belgian Commission de la protection de la vie privée, Recommandation n° 01/2013 du 21 janvier 2013, https://www.privacycommission.be/sites/privacycommission/files/documents/recommandation_01_2013_0.pdf.

CNIL, Recommendations for companies planning to use Cloud computing services, http://www.cnil.fr/fileadmin/documents/en/Recommendations_for_companies_planning_to_use_Cloud_computing_services.pdf

CSI-SLA Subgroup (European Commission), "Cloud Service Level Agreement Standardisation Guidelines", 2014, https://ec.europa.eu/digital-agenda/en/news/cloud-service-level-agreement-standardisation-guidelines.

Data Sharing and Tracking of Transactions in the Banking Sector, Decision by the Italian DPA of 12 May 2011 as published in Italy's Official Journal no. 127 dated 3 June 2011, http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1868766.

IG Toolkit Incident Reporting Tool https://www.igt.hscic.gov.uk/resources/IG%20Incident%20Reporting%20Tool%20User%20Guide.pdf.

Marnix Dekker and Christoffer Karsberg 'Technical guidance on the incident reporting in Article 13a' (ENISA, November 2013)

Marnix Dekker, Christoffer Karsberg 'Technical guidance on the security measures in Article 13a' (ENISA, November 2013).

Marnix Dekker, Dimitra Liveri, Matina Lakka, 'Cloud Security Incident Reporting - Framework for reporting about major cloud security incidents' (ENISA, 9 December 2013)

OECD (2015), Digital Security Risk Management for Economic and Social Prosperity

OECD Recommendation and Companion Document, OECD Publishing, Paris. DOI: http://dx.doi.org/10.1787/9789264245471-en

OECD, Recommendation of the Council concerning Guidelines governing the protection of privacy and transborder flows of personal data, 11 July 2013, available at: http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf

OECD, Recommendation of the Council concerning Guidelines governing the protection of privacy and transborder flows of personal data, 23 September 1980, available at: http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

Privacy Commission of Canada, Getting Accountability Right with a Privacy Management Program, https://www.priv.gc.ca/information/guide/2012/gl_acc_201204_e.pdf.

Rettifica alla Deliberazione n. 513 del 12 novembre 2014 recante 'Provvedimento generale prescrittivo in tema di biometria' - 15 gennaio 2015 (Pubblicato sulla Gazzetta Ufficiale n. 34 dell'11 febbraio 2015), http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3556992.

UK ICO, Guidance on data security breach management (2012), https://ico.org.uk/media/for-organisations/documents/1562/guidance_on_data_security_breach_management.pdf

UK ICO, Notification of data security breaches to the Information Commissioner's Office (2012), https://ico.org.uk/media/for-organisations/documents/1536/breach_reporting.pdf