CLOUD ACCOUNTABILITY PROJECT

D:B-5.2 Report on legal and regulatory dependencies for effective accountability and governance

Deliverable Number:	D25.2
Work Package:	WP 25
Version:	Final
Deliverable Lead Organisation:	QMUL
Dissemination Level:	PU
Contractual Date of Delivery (release):	30/09/2014 (Extension agreed with PO to 12/11/2014)
Date of Delivery:	12/11/2014

Editors
Brian Dziminski (QMUL) Chris Reed (QMUL)

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

Reviewer(s)
Tomascz Wiktor Wiodarczyk (UIS) Slani Pearson (HP) Amy Holcroft (HP)

Table of Contents

Executive Summary

This deliverable is the final output from work package 25, Contractual and Regulatory Considerations. It aims to explain the complex legal and regulatory landscape of requirements that dictate how actors in the Cloud ought to behave, to analyse how accountability tools can interact with law and regulation, and indicate the policy and governance processes which are required to close the accountability loop.

The deliverable is divided into seven substantive parts:

Section 2: a general overview of the law making process, with a primary focus on the EU and the US, the two primary jurisdictions impacting Cloud providers and users.

Section 3: an examination of jurisdiction and choice of law, and how such issues impact Cloud users, customers and providers.

Section 4: a review of the data protection and privacy laws which impact use of the Cloud and are the main focus of A4 Cloud.

Section 5: the role of contracts in the Cloud, an equally important legal aspect of the Cloud.

Section 6: an explanation of how the law provides remediation and redress for compliance failures.

Section 7: an analysis at a conceptual level of the role which accountability tools can play in demonstrating some levels of compliance with law and regulation.

Section 8: an examination of legal governance and the development of policy framework for companies conducting business in the Cloud, and how the development, enforcement and adaptation of such policy can increase accountability in the Cloud.

From our analysis we draw four conclusions:

1. Although the law and regulation which applies to data protection and confidential information in the cloud is highly complex and changing, the fundamental principles of the law are clear and simple. Accountability therefore needs to focus most strongly on demonstrating that the fundamental principles of law have been complied with. As a Cloud business's activities increase in scope and range, so should the layers of accountability it provides and the information contained in those accounts.

2. Accountability methods and tools can play an important part in achieving accountability by revealing the internal workings of Cloud activities so that legal and regulatory compliance can be assured. To this end, it is important that those methods and tools be designed so as to assist the legal and regulatory compliance process and provide the information that process needs.

3. Accountability tools are one part of a larger mosaic, which has to include mechanisms for development of policy and governance processes which ensure that policies are appropriate to achieve compliance and are actually put into effect.

4. Law and regulation should be designed with accountability in mind, so as to secure the advantages in terms of compliance which accountability makes possible.

1 Introduction

This deliverable is the final output from work package B5, Contractual and Regulatory Considerations. The White Paper on the new data protection framework, D B-5.1 has analysed in depth the existing data protection law framework as it applies to Cloud accountability, and how the proposed data protection Regulation would change the legal and regulatory position. The intended audience for that White Paper was primarily lawmakers, regulators and practising and academic lawyers. The purpose of this deliverable is very different.

Its first aim is to conclude work package B5 by providing a comprehensible overview of the wider legal and regulatory environment within which the A4Cloud methods and tools will have to operate. These methods and tools are mechanisms through which Cloud stakeholders can be aided to become accountable for the privacy and confidentiality of information held in the Cloud. Their outputs do not make stakeholders accountable per se, but instead need to be used by those stakeholders in ways which enhance accountability. It has become clear through the interactions between the different work packages that detailed and granular legal analysis has the potential to obscure the issues which those methods and tools need to address, rather than illuminating them. A primary purpose of this deliverable is therefore to provide the information which the other A4Cloud partners need to develop and refine the concept of accountability and to produce the accountability tools which are the final output of the project.

Its second aim is to provide guidance to Cloud providers, businesses utilizing the Cloud, and, to a lesser, yet still important extent, European consumers using the Cloud. To this end we explain the applicable laws in simpler terms, so as to provide guidance to those segments of the Cloud community in a more understandable fashion than is presented in the majority of legal scholarly writing. This is one of the primary goals of A4Cloud.

This deliverable therefore focuses on two audiences:

(a) Those whose role it is to develop and deliver accountability, both within A4Cloud and more widely. These persons require a deep understanding of the legal and regulatory dependencies, but at a comparatively high conceptual level rather than at the granular level at which lawyers work. They also need to understand the wider context in which the specific legal and regulatory topics of A4Cloud are situated, and thus this deliverable explains the wider framework, including how jurisdictional uncertainties affect accountability, how other relevant areas of law such as consumer protection fit in, and how the EU regime sits within its global legal and regulatory context. This, we believe, will greatly assist those partners in their ongoing development of the technical tools in the A4Cloud Project.

(b) The wider community of cloud providers and customers, who should be considering accountability and therefore need to understand the legal and regulatory considerations concerned.

The legal and regulatory dependencies for cloud computing derive from two primary sources: (1) relevant laws and regulations, which most notably include the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data Official Journal L 281, 23/11/1995, pp. 31 – 50. (Hereafter referred to as the 'Data Protection Directive' and/or the 'DPD'); and (2) contracts between the various users of cloud computing, which necessarily includes agreements, privacy notices, privacy policies, and other terms and conditions utilised by cloud providers. However, as explained throughout, there are other laws which greatly impact the Cloud context and which Cloud providers and Cloud customers should be aware.

Importantly, many of the regulatory dependencies are in a state of flux, in particular the DPD. The proposed regulation to supplant the DPD (the "Regulation"), is still in the process of agreement. Once enacted it will change many of the rules under which cloud actors currently act. The meaning of the legal rules is also subject to constant clarification through decisions of the Court of Justice of the

European Union. Its opinions refine and extend the interpretation and application of data protection law.[1] Law and regulation is a moving target.

In light of the foregoing and in furtherance of our goals, this deliverable is split into three general areas. Sections 2 to 6 of this deliverable provide a general overview of the legal and regulatory dependencies. This starts in sections 2 and 3 with a high-level look at the legal process, including examining the jurisdictional issues which greatly impact cloud computing. Law is primarily territorial in scope, which means that an activity like cloud computing which spans multiple jurisdictions attracts the attention of laws from all those jurisdictions. Section 4 explains the most important specific laws which impact the Cloud, including the DPD, the proposed Regulation, and other regulations, including those of the US and other jurisdictions. Section 5 examines contracts in the Cloud, and how such contracts also control the relationships of cloud actors. Finally, section 6 explains the remedies available to cloud actors when there is a privacy breach.

The second conceptual element of this deliverable, section 7, attempts to explain how accountability tools interact with legal and regulatory compliance. Legal rules are particularly resistant to computation because of their complexity and constant change, the fact that their meaning changes with context*, and their numerous requirements for the exercise of human judgment. The dominating laws of data protection, trade secret protection, and contracts are particularly resistant. This section summarises the results of some 40 years of theoretical research into this problem, and attempts to explain how the tools being developed by A4Cloud can be integrated into the compliance process so as to produce accountability.

The final portion of the deliverable, section 8, discusses governance and policy for businesses conducting business in the Cloud and Cloud providers in light of the state of the law. The tools being developed in A4Cloud need to be supplemented by appropriate governance and policy if the aim of protecting personal data and/or sensitive business information is to be achieved. Thus, we take a pragmatic approach to accountability in examining what steps such businesses should take in increasing accountability within their organisations. In doing so, we examine how businesses must first start with understanding the regulatory and contractual provisions that control the relationship with customers and consumers. Businesses must then conduct a risk assessment to better evaluate what measures they should take based on the threat, vulnerability and expected loss associated with any data breach. Then, we examine the next step Cloud businesses must take in establishing policy, internal standards, and deciding on the tools which should be utilised, including those being developed in A4Cloud, to minimize the threat and exposure of data breaches. Next, we see that that businesses cannot just establish policy, but they must enforce that policy and adapt to the ever-changing nature of not only the regulatory and legal considerations controlling the Cloud landscape, but the equally ever-changing technological landscape, both as to risk and as to security. Finally, we examine what Cloud businesses should do when there is an incident and how businesses should handle breach notification.

As an outcome of this deliverable, it is expected that the intended audiences will gain a better understanding of the legal landscape of the Cloud and how the partners in A4 Cloud, and Cloud providers and businesses utilising the Cloud can better approach these issues and ultimately increase accountability throughout the Cloud.

* As a simple example, the same item of data can be personal data in the hands of person X, but not personal data in the hands of person Y, depending on the other information which those persons possessor have access to.

2 General overview of the law

We live and conduct business in a world of very complex laws. Understanding the law is complicated by the fact the laws are constantly revised as result of their interpretations by courts, regulators and other enforcement bodies, Compliance with such laws one month may not mean compliance the next. Courts also apply such laws inconsistently leaving those subject to the laws to oftentimes partaking in a guessing game about what the laws really mean and how they will be applied in any given situation. And, what is perhaps the proverbial icing on the cake, the nature of the Cloud, i.e. doing business across the Internet and Cloud providers being able to provide services without physically being within a jurisdiction, adds a whole new layer to the legal quagmire in determining which laws apply in any given transaction.

In other words, the legal landscape as it applies to the Cloud is in many ways quite cloudy itself.

2.1 The development of modern law

Nevertheless, we start with the basics. Most of today's laws have their roots in the move from absolute monarchy to the recognition of individual rights, as exemplified by the Magna Carta signed 800 years ago and the human rights laws derived from that charter. The Magna Carta was drafted and imposed upon King John of England to provide certain liberties to his subjects and for the King to accept that his will was not arbitrary, but rather that people could only be punished by the rule of law.

Flash forward eight centuries, and the world has evolved to 196 countries, each with its own sets of law, and many of those having different state or federal laws within the country. Within those countries, there are two primary systems: common law and civil law. Common law jurisdictions are generally uncodified, meaning that there is no comprehensive recitation of statutes or codes, and instead law is primarily developed through judicial decisions which establish legal precedent over time. On the other hand, civil law jurisdictions follow a system of law that is codified, meaning that such jurisdictions have comprehensive recitations of codes attempting to envision the potential application of those codes to different scenarios that courts must then follow. In these jurisdictions judicial decisions are less important in future applications of the codified laws. Finally, within both systems, there are different sets of laws that primarily fall into private law (for our purposes, contract and torts (a civil wrong not arising from a breach of contract) are the most important subsections of private law, or public law (which also encompasses criminal laws, but importantly for our purposes also contains such laws as data protection laws).

Law, whether common law or civil law, can ultimately be summed up in two basic concepts. The first is 'complicated.' Each of the 196 nations desires those laws to protect its citizens and therefore has an inherent interest in broadly applying those protections. For example, the U.S. has federal laws which will generally apply to any companies doing business within the U.S., i.e. targeting their activities to U.S. citizens residing in the U.S.[*] Under that federal law system, there are hundreds of District Courts interpreting and applying those laws, thirteen Circuit Courts of Appeals serving as appellate courts for appeals from those District Courts, and ultimately, the U.S. Supreme Court also reviewing various cases from the Circuit Court of Appeals, especially when those courts decide similar issues differently or when laws are deemed to be unconstitutional. And that is just the federal level of the U.S. concurrently with those federal laws, there are fifty states, each of which has their own set of laws. And, while many of those laws mirror the federal laws and are similar throughout the fifty states, there are nevertheless enough differences to trip up even the most savvy of businesses, users, and, oftentimes, even lawyers. Those fifty states usually have dozens, and sometimes hundreds, of courts, their own appellate courts, and their own courts of final jurisdiction similar to the U.S. Supreme Court, applying such laws, oftentimes again with little to no indication how the ultimate determinations as to any given law will be decided.

[*] The concept of 'targeting' is discussed in greater detail below in respect to jurisdiction, but generally encompasses when a business intentionally directs its business to citizens of a state.

In the European Union (EU), there are 28 different member states and a complicated legal framework of laws which emanate from the European Union's law making institutions and directly apply within those states (such as Regulations), other laws which Member States are obligated to enact through local laws which allows a degree of interpretation (such as Directives). In other areas of the law Member States are free to enact their own legislation or stricter legislation than required at European level and often with little to no guidance from the EU. Outside the domain of EU competence, member states have their own laws which might be relevant to cloud accountability, and these can diverge radically. An important example for this deliverable is the law of confidential information and trade secrets, which is different in each member state. A proposal for a directive on this matter is currently under consideration[2], but if adopted it will only harmonise part of the law, leaving the rest with national law differences.

The ultimate conclusion from the foregoing is it is nearly impossible for a Cloud provider to comply with all of the laws that may be applicable, especially when many of those laws are in conflict, for example, where one country or law may require that records must be maintained for a certain period of time where another law may require that records be deleted within the same time parameters. Thus, again and to say the least, laws are complicated.

The second concept to describe our international laws is uncertainty. Ask any lawyer or legal scholar a question as to a hypothetical or real situation and how the decision of law will be applied, and you most certainly will be met with a response in the vein of "it depends." Lawyers will ask more questions about the facts, want more details, and even when you have all those answers, the lawyer's advice may still be dependent on other undiscovered facts, the laws which might or might not apply, how a court applies the law, and, in some jurisdictions and/or cases, how a jury views and decides the facts in question. This can be very frustrating for anyone having to deal with such laws, especially where there are serious implications for failures to comply. This becomes even more heightened in the Cloud, as not only are Cloud actors faced with trying to decide which laws are applicable but are then faced with uncertainty as to the application of those laws. This leads to laws adopted to cause one specific consequence creating opposite and/or other unintended consequences, including many companies consciously deciding to not comply with certain laws (generally making a risk assessment of where they might face jurisdiction, discussed in greater detail below, or minimal sanctions or penalties) or companies deciding to not to do business at all in some jurisdictions. But, the most common result is companies do what they can to comply in spirit in order to still conduct business, but hopefully avoid any consequences for any non-compliance with any given law.

2.2 How laws are generally made

Most laws generally arise from human rights, social norms, economic necessities, and the necessary protection of society and citizens. How such laws are made in any given country or state may vary greatly, but most democratic states follow systems similar to that of the EU or US, the two most important jurisdictions in our review of Cloud Computing law.[*]

In the European Union, there are three main decision-making institutions involved in the law-making process: the European Parliament, the Council of the European Union, and the European Commission.[†] Together, those three institutions produce the policies and laws that apply in varying degrees throughout the EU Member States depending on the type of law adopted. The process is very time-consuming, complicated, and oftentimes politically charged. One prime example is the data protection laws discussed in greater detail below and the ongoing attempt to adopt a Data Protection Regulation to

[*] As a project that is partially funded by the European Commission, A4Cloud is primarily focused on EU law, especially the Data Protection Directive and proposed Data Protection Regulation. However, many of the companies doing business in the EU are companies organized under US law and the contracts being utilized, and/or terms and conditions of the use of such services is oftentimes governed by US law. Thus, examination of US law, at least in relevant part, is as equally important as many of the EU laws impacting the Cloud.

[†] There is also the Court of Justice of the European Union which decides cases involving EU laws after referral and cases between Member States, and whose decisions can impact the future application of such laws, but which does not otherwise participate in the lawmaking process.

replace the current Data Protection Directive.* Such attempts have been ongoing for some years now, and yet remain in a relatively early stage of the process which is only complicated further by elections and changes in the European institutions noted above. Oftentimes this leads to legislation being scrapped or having to be taken back to an earlier stage in the legislative process.

In the U.S., laws are enacted at both the federal level and at the state level. The federal law-making process consists of three branches of government in the legislative branch (Congress), executive branch (the President and federal administrative agencies), and the judicial branch (federal courts). In its simplest of functioning, the legislative branch enacts the laws, the executive branch applies the laws, and the judicial branch interprets the laws (which as a common law jurisdiction can supplement, refine, and/or even void enacted laws). Most of the fifty states follow a similar process in adopting their own laws and, like the EU, the U.S. lawmaking process is very time-consuming and politically charged.

2.3 The role of courts

The role of the courts deserves some special attention, as that is where parties will most often be looking be for their remedy. As referenced above, the courts play a critical role in developing the law in common law jurisdictions. When litigating a dispute, the decision will lie in the hands of a judge, a panel of judges, or, in some jurisdictions, a jury. And, as decisions get appealed, those cases will advance to higher courts, and the decisions made at those courts will usually have binding effect on the courts below. Generally the decisions of the highest courts will be binding on all courts below.

A case relevant to accountability in the Cloud provides a good example of this process in the European Union - Google Spain v. AEPD.[3] Unlike a case that gets appealed up through the system of higher courts, the Google Spain case was one in which a preliminary ruling was requested from the European Court of Justice by Audencia Nacional (National High Court) of Spain. The preliminary ruling procedure allows a national court which is in doubt about the interpretation or validity of an EU law to ask the European Court of Justice for advice. The advice given by the European Court of Justice is in the form of a preliminary ruling, which is then binding on courts in all EU Member States.

In this case, the National High Court of Spain requested a preliminary ruling on questions of the territorial application of the Data Protection Directive; whether Google acted as a controller through the provision of an Internet search engine; and whether a citizen had a right to demand the erasure of information otherwise lawfully published and found through internet searches. The European Court of Justice issued a preliminary ruling finding that Google Spain had set up a subsidiary in Spain and was therefore subject to the Data Protection Directive; that Google Spain was a controller through the process of finding information, indexing that information, temporarily storing the information and then making that information available to the searcher; and that citizens had what is commonly referred to as a "right to be forgotten" pursuant to the DPD (i.e. to have links to data about them erased from the search engine results).[4] Now, as set forth above, this controversial decision binds all EU Member States reviewing similar issues in the future. This decision is illustrative of both the preliminary ruling procedure impacting all courts in the EU and how the interpretation of the DPD and expectations of many scholars, lawyers, and pundits as to how the European Court of Justice will rule, can be entirely wrong. This all serves to highlight the uncertain nature of the legal process.

* The difference between a Directive and a Regulation is an important one, especially with the current posture of the data protection framework. A Directive is a law that each Member State must enact, but the Member State has discretion in how the law is made effective and generally such laws do not need to be enacted for many years after adoption. To the contrary, a Regulation is directly applicable and enforceable in all Member States. As seen below, the EU is attempting to transform the current Data Protection Directive into a Data Protection Regulation.

3 Jurisdiction

Having outlined how the laws are made, and what those laws actually provide, the next step is to understand to who and how those laws apply to persons and legal entities. This concept can be summarized as jurisdiction, which for our purposes includes what laws will apply to any given situation and where a dispute will be adjudicated, also known as venue. Such determinations can be as complicated as the lawmaking process itself and present two general questions in respect to the Cloud: (1) can a state apply its public law to a foreign business, and if so, when and under what circumstances; and (2) in a private dispute, which laws will apply and which Court has the power to adjudicate that dispute?

3.1 General overview of jurisdiction

In respect of the first question, a state's laws always apply to those who are within the state's geographical territory. But it is common for laws also to apply to those outside the territory if their activities affect the state in some way. Determining the extra-territorial jurisdiction of public law is guided by two overriding principles. The first is comity, in that a state should not regulate an activity where it is more appropriate for another state to do so. The second is the effects doctrine, in that a state may regulate a foreign activity which has effects in its territory. That brings us back to the basic underlying problem with the Cloud – when and where is it appropriate for a state to regulate a Cloud provider? Answering those questions leads to more questions, some of which are answered and addressed below in further examining some of the rules and regulations in respect to jurisdiction. More notably and quite problematic, is that when states are perceived to have overstepped their bounds, such excessive authority claims by states can lead to problems such as legal enforcement becoming more difficult, if not impossible, based on other states refusing to cooperate with such enforcement; it can also foster a culture of evasion by businesses and citizens of not only the laws in question, but also other laws; it can dilute the otherwise normative effect of law (again, even with other laws which were not originally the subject of the excessive authority claim); and, ultimately, it can create a conflict between states (which has been seen to some degree between the US and the EU in respect to the Data Protection Directive and some of the restrictions in EU law regarding transborder transfers of data, discussed below).[5] Again, all of these problems are especially common in the Cloud by virtue of business being conducted in a multi-locational Cloud which is not located in one given state. The Data Protection Directive purportedly answers that question in respect to EU Member States' governance of data protection issues, though, as seen below, it again raises more questions and the answers may not be as clear as they first seem.

3.2 EU Jurisdiction

The EU has three main legal instruments which are relevant to the assertion of jurisdiction.[6] The first is the Brussels Regulation, which generally applies to consumer contracts and provides that a consumer may sue within his or her own jurisdiction, regardless of what the contract otherwise states. The second is the Rome I Regulation, which decides which state's law applies to contracts, and for most situations provides that the law of a consumer's residence will apply if the merchant has directed its activities to that state, but that a choice of law provision contained within a contract is enforceable if it does not derogate from any protections provided under the consumer's national law. Finally, the Rome II Regulation applies in respect to torts and generally provides that the applicable law will be that of the state where the harm occurred. Though these regulations provide some semblance of clarity as to the exercise of jurisdiction, they are not always clear-cut. It is usually only possible to work out how they apply after the problem has arisen, rather than in advance, and difficulties can arise in answering questions like what constitutes a merchant directing their activities to a state and what constitutes harm in some cases and determining where that harm 'occurs.'

3.3 U.S. Jurisdiction

In the U.S., there are two types of jurisdiction that must be present for a federal court to exercise jurisdiction.[*] The first is subject matter jurisdiction, meaning that either some federal law specifically applies or that a dispute is between two citizens of different states, or a different state and different country. The second is personal jurisdiction, meaning a party must have availed itself to the protection of the laws of the U.S. and have minimum contacts with the jurisdiction in question, generally a specific state.

In respect to the Cloud, the decision and test provided in *Zippo Manufacturing Co. v. Zippo Dot Com, Inc.*[7] remains rather instructive. The court in the *Zippo* case held that courts should apply a sliding scale where purely passive operators will not be subject to personal jurisdiction, whereas active websites (similar to the targeting test of the Rome I Regulation in the EU) will be subject to jurisdiction. This test, while not binding on other courts as it was decided by a Pennsylvania District Court and therefore has no impact outside of that court, has nevertheless been widely accepted in reviewing situations involving internet companies, web companies, and now the evolution into the Cloud. However, as can readily be recognized, most Cloud companies will fall somewhere in the middle, leading to a complicated and fact-intensive analysis all leading back to the answer of "it depends" discussed above.

3.4 Implications of jurisdictional issues on cloud computing

This overview was not intended to scare the reader and make one avoid the Cloud altogether. Rather, this overview introduces some of the basic concepts of law which Cloud actors should consider and be aware of in conducting business and are which strong building blocks in looking at some of the issues below in respect to data protection laws and Cloud contracts. Nevertheless, as seen, some of these concepts are quite complicated and Cloud actors should proceed with caution and diligence in undertaking business in the Cloud to ensure proper compliance. Dealing with these concepts will be explored in greater detail in Section 5 in discussing effective legal governance and accountability from a legal perspective.

[*] Most states follow similar principles in regard to the exercise of jurisdiction under state constitutions and laws.

4 Primary regulations impacting Cloud computing

As noted in the Introduction, A4Cloud is most concerned with two legal areas: data protection laws and contracts. Generally speaking, the approach to data protection varies around the globe. The EU has taken a paternalistic approach in adopting the Data Protection Directive in 1995.[8] As seen below, that Directive strives to provide a comprehensive framework to protect a person's personal information, with state-established bodies charged with enforcing the law. Meanwhile, the US has does not have a comprehensive privacy law but has adopted sectoral laws most notably in the financial and health care sectors and the Federal Trade Commission, as well as similar state administrative agencies and/or attorney generals, have undertaken some efforts in protecting privacy rights through its enforcement powers where companies have been alleged to engage in deceptive trade practices. Finally, some states have followed the EU model (countries such as Canada and many Latin American countries); other states have followed a sector-based approach like the U.S. (countries such as Japan); other states have followed more of a self-regulatory scheme (countries such as Australia and New Zealand); and other states have not enacted much protection at all (countries such as China).[9]

In the following review of the data protection law applicable to Cloud we have focused on some of the more significant of those laws and regulations, while also giving a brief overview of others which we think should be considered and which business utilising the Cloud should be aware of. We provide this overview of the legal and regulatory dependencies by primarily examining the EU, but also by looking at the important regulations in the U.S., as well as a brief look at how some other jurisdictions are handling the biggest issues impacting accountability the Cloud. As the reader would probably expect, the biggest area of law impacting accountability are the data protection and privacy frameworks throughout the world. Beyond those laws, the next important area of the law, at least in the A4Cloud approach, are laws governing sensitive business information and trade secrets. Finally, there are other laws which should be considered, including consumer protection laws and some other laws geared specifically towards to internet technology. As noted, this is not a comprehensive review of all laws impacting Cloud computing, but should provide a solid start for most businesses and Cloud providers.

4.1 European Union laws

4.1.1 The Data Protection Directive and proposed Data Protection Regulation

This section of the deliverable provides an overview of the main EU data protection legislation and the key concepts in EU data protection law. This focuses on the current EU Data Protection Directive 1995. It then discusses the difficulties with applying data protection law in a cloud environment.

4.1.1.1 Origins of EU data protection law

Nearly 100 countries worldwide currently have laws regulating personal data. Technological advances in the twentieth century enable the manipulation of data in a variety of different ways with an increasing capacity to process, store, search and analyse personal data, especially with the ever-increasing attention, use and value of 'big data.'*

* The term 'big data' is generally used to describe collections of large data sets, oftentimes so large that it is difficult to process using traditional software and/or database technology.

Data protection laws have their origins in a recognition of a right to privacy. All EU Member States are signatories to the European Convention on Human Rights (ECHR) that recognises in Article 8 a right to privacy. This right has been re-stated in the EU Charter of fundamental freedoms as the right to respect for private and family life (Article 7) and supplemented by a specific right to the protection of their personal data (Article 8). Ultimately, various harmonisation measures in Europe on data protection such as the 1980 OECD guidelines (updated 2013) and the Council of Europe Convention in 1981, led the European Commission to propose EU legislation to harmonise diverging data protection legislation in EU Member States. The EU Data Protection Directive, adopted in 1995, is the key piece of legislation on data protection which has been implemented through local law in all EU member states. On 25 January 2012 the European Commission unveiled a proposed legislative reform of the current data protection law in the EU that would replace the Data Protection Directive by a General Data Protection Regulation[10]. At the time of writing there is no predicted date by which the reform will be completed and this review has focused on the current law which is likely to be in place until at least 2016. The underlying purpose of the General Data Protection Regulation was to better define responsibilities and to increase accountability:

> The proposals place clear responsibility and accountability on those who are processing personal data, throughout the information life cycle. In the Regulation, we have included incentives for controllers to invest, from the start, in getting data protection right. For example, we have foreseen data protection impact assessments, data protection by design and data protection by default, which will encourage data controllers to think about data protection from the very beginning when designing new applications or services. We have also clarified and strengthened citizens' rights. We clarify the notion of consent, introduce a general transparency principle and enhance redress mechanisms. And we introduce an obligation to notify clients or users in the event of a data breach which will apply to all sectors.[11]

One feature of the current EU data protection law is that as it is a Directive, member States are required to implement the Directive into national law and they have discretion on how it is implemented which has resulted in the laws varying in member states, in some cases being stricter than the Directive, and there being only a minimum level of harmonisation in the laws across the union.

4.1.1.2 Main concepts

The Directive regulates the processing of personal data, irrespective of whether such processing is automated or not.

Scope of personal data
Personal data means data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller. This includes any expression of opinion about the individual.[12]

Sensitive personal data is a special category of personal data that is subject to stricter regulation.[13] Sensitive personal data relates to specific categories of data which are defined as data relating to a person's racial origin; political opinions or religious or other beliefs; physical or mental health; sexual life; criminal convictions or the alleged commission of an offence; trade union membership. There are more safeguards for sensitive personal data, due to the fear of it being used to discriminate against groups of people and the potential privacy loss if it is misused. In most cases a person must be asked for their consent to the collection and processing of sensitive personal data can about them.

The distinction between data processors and controllers in EU data protection law
The law protects the rights of individuals whom the data is about, called data subjects, mainly by placing duties on those who decide how and why such data is processed, called data controllers.

A data controller is a person or company that collects and keeps data about people and 'determines the purposes and means of processing of personal data'.[14] The data controller has the main responsibility for complying with data protection legal obligations. A data controller must ensure that the processing of personal data complies with certain principles. These require that personal data must be processed fairly and lawfully for specified lawful purposes only. The processing must be adequate, relevant and

not excessive. Personal data must also be updated as necessary, accurate and not kept longer than required. It must be processed in accordance with data subject rights.

The data processor is a 'natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller'.[15] Unlike data controllers, data processors do not have obligations in law concerning security of data processing.[16] While the controller is required to implement measures against, amongst other things, accidental or unlawful destruction or accidental loss of data, processors do not have any direct obligations to ensure data security. Instead, the law requires the controller to ensure that the contract with the data processor obligates it to only process data on the instructions of the controller and to implement appropriate security measures to protect the data. Under the proposed Regulation data processors would be directly subject to extensive obligations.

This distinction between data controllers and data processors is an important distinction because they are treated differently under the Directive, with responsibility and liability ultimately falling upon the data controller. Data controllers must ensure that any processing of personal data for which they are responsible complies with the law. Failure to do so risks enforcement action, even prosecution, and compensation claims from individuals.

Data processors on the other hand are not otherwise subject to the law because they are presumed to be just following data controllers' instructions. Data processing means performing any operation or set of operations on data, including**:** obtaining, recording or keeping data, collecting, organizing, storing, altering or adapting the data, retrieving, consulting or using the data, disclosing the information or data by transmitting, disseminating or otherwise making it available, aligning, combining, blocking, erasing or destroying the data.

Data controllers remain responsible for ensuring their processing complies with the law, whether they do it in-house or engage a data processor. In law, a data controller who chooses to 'outsource' data storage or processing remains a controller and responsible for complying with the Data Protection Directive. If problems arise from third party failures, the controller is still liable.

As data processing activity becomes more complex, applying the distinction between data processor and data controller has become more and more difficult.[17] At first sight it might appear that a cloud provider will never be more than a data processor, and arguably not even that in some instances.[18] But to the extent that the Cloud provider determines *some* of the "purposes and means of processing" it may be a data controller, even if it acts as a data processor for other of its activities.

Principles of data protection

In order to process data in compliance with the Directive, controllers must comply with the following principles:

Collection & use of personal data

Article 6(1)(a) of the Directive requires that personal data is "Processed fairly and lawfully". Fairness of the purpose of collection and intended uses. "Fairness" depends on one's perspective, and courts tend to interpret it from the data subject perspective. In addition, pursuant to Article 6(10(b), the data must be processed "for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes." If the data controller wishes to process data for an incompatible purpose to that originally notified to the data subjects, they must re-notify. This presents compliance challenges for data controllers as technological advances facilitate the collection of increasing quantities and new potential uses for that data become possible and, potentially, desirable to one or more of those concerned*, for example via data mining and other Big Data analytics techniques.

Legitimate Processing Criteria

* Analysis of this kind can offer individual or even public benefits (see eg http://www.technologyreview.com/view/526471/how-to-detect-criminal-gangs-using-mobile-phone-data/) as well as benefits to the controller.

Article 7 of the Data Protection Directive sets out certain criteria on which a data controller must base its processing activity in order for it to be legitimate. These criteria are consent, necessity, contract requirement, legal obligation, protection of data subject, public interest and legitimate interests of the controller. Consent of data subject is the most often cited. It is not merely consent but *specific and informed consent* that is needed. It is easy now to get 'tick box' consent, particularly online, but more difficult to show informed consent. Contractual necessity means that the processing is necessary to perform the contract, for example: billing information about the customer, the company will need to process name, address and details of payment in order to fulfil the customer's contract. Legitimate interest is perhaps the most common justification for data processing, which requires that the processing is necessary for the legitimate interest of the data controller provided that interest is not overridden by the fundamental rights and freedoms of the data subject.

Application of the Law

The EU Data Protection Directive applies when the data controller is established within the EU, which for foreign controllers means that it has a subsidiary, branch or agency with in the EEA.[19] It also applies when the controller is in a place where a member state's national law applies by virtue of international public law (e.g. in a ship or aircraft flying a particular Member States' flag).[20] Finally, it may apply to a data controller that is not established in the EEA but that makes use of equipment/means situated in the EEA for the purposes of processing personal data.[21] The national laws implementing the Data Protection Directive are not harmonized and implementations differ. This means that the provisions on jurisdiction are subject to interpretation. Potentially any online business dealing with EU customers could be found to be processing personal data via EU-located equipment/means (such as cookies stored on the customers' computer[22]) and therefore subject to EU data protection law. The proposed reform to the law (i.e. the EU General Data Protection Regulation) plans to extend the scope of jurisdiction to anyone processing personal data of EU residents or targeting EU residents through data tracking, mining and targeted advertising. This facilitates the extraterritorial application of EU law, but is intended to ensure that EU data protection laws cannot be avoided by processing data outside the EEA. As regards cloud computing, the new Regulation needs to clarify whether EU data protection laws could apply to the use of EEA data centres or EEA cloud providers particularly where layers of providers are involved and when processing personal data from non-EEA controllers. Any legal uncertainty over jurisdiction could discourage non-EEA entities from using EEA data centres or from using EEA Cloud providers.

Sending Personal data abroad

Article 25 of the Data Protection Directive restricts the transfer of data outside the EEA.

Personal data can be transferred freely to countries within the European Economic Area but transferring data to a country or territory outside the European Economic Area is only permitted if that country or territory ensures an adequate level of protection for the rights and freedoms of individuals in relation to processing personal data. The European Commission can declare that certain countries provide adequate protection and data can be freely exported to those countries in what are known as "findings of adequacy".[23] Relatively few countries feature on this list[24], which includes special arrangements for transfers of data under the EU-US Safe Harbor Program.

In respect of transfers of data to the U.S., the U.S. and EU have agreed a self-regulatory regime that applies to transfers of data to US organisations, including cloud providers. An organisation can show an adequate standard of data protection as required by EU data protection law by becoming certified under the EU-U.S. Safe Harbor Program. The U.S. Department of Commerce developed this program in consultation with the European Commission and allows US companies to self certify as having an adequate level of data protection and consequently allows EU based data controllers to transfer data to them. Apparently the popularity of this program has increased with the advent of cloud computing.[25]

Another way to comply with the transfer restrictions is to use model contracts with standard contractual clauses, the terms of which have been approved by the European Commission for transfers of data outside the EEA.[26] The European Commission has issued clauses for transfers of personal data from an EEA-established controller to a controller in a third country or from an EEA-established controller to a third-country processor.[27]

Binding Corporate Rules (BCRs) are codes of conduct dealing with international transfer of personal data within the same group of companies, within a multinational company.* They are subject to approval by relevant national data protection authorities and this process can be long and costly. Controller BCRs only allow transfers within the same corporate group, so they might be helpful to make data transfers within a group's private cloud, but it cannot be used if a cloud provider or sub-provider is outside the corporate group.[28] BCRs for processors were introduced in 2012 and, once a BCR for processors is approved it can be used by controllers and processors to ensure compliance with EU protection rules.[29] The requirements for approval for processor BCRs mean that it can only be used in a limited number of situations in cloud computing and is unlikely to be used where providers use sub-providers or do not control the supply chain. Because the aim of BCRs is to replicate the legal effect of the Directive's provisions through rules about data processing and transfers which are binding as between the members of a corporate group, drafting the rules is a complex and length activity. The costs in management time and legal advice make BCRs unattractive to all but the largest corporate groups.[30]

Supervision and Enforcement

National data protection authorities† were required to be set up by the Data Protection Directive.[31] They have three core powers: investigative powers, effective powers of intervention and power to engage in legal proceedings. They are required to receive and deal with complaints and required to provide annual reports that are made public. They also play a role in giving guidance and recommending changes to the law.

Supervisory authorities on data protection law include the European Data Protection Supervisor which is an independent supervisory authority to ensure that European institutions and bodies respect data protection law. In addition, there is a body that brings together all the EU data protection bodies: the Article 29 Working Party.‡ The Article 29 Working Party is made up of representatives of the data protection authority of each EU Member State, the European Data Protection Supervisor and the European Commission. Its main role is to give advice to the Member States on the interpretation of the data protection directive and to achieve harmonious application of the data protection directive in the EEA. It also gives the European Commission an opinion on the laws that impact on data protection law. Although its opinions and advice are non-binding, they are highly influential as guidance on how data protection laws will be interpreted and applied by European Data Protection Authorities (DPAs).

Although this appears to be a vast system of data protection authorities, the reality is that the variations in national implementation of the Data Protection Directive and the lack of harmonisation between Member States has meant that there is a patchy data protection regime and, in some Member States, little enforcement of data protection law. Nevertheless, since 2011, there has been a steady rise of cloud investigations conducted by European DPAs and this trend is predicted to continue.[32]

4.1.1.3 The Cloud and data protection

Cloud computing raises particular questions with regard to how data protection laws apply to personal data in the cloud. The implications of data protection law on cloud computing can be analysed based on the answers to four questions:[33] What information in the Cloud is 'personal data'? Who is responsible for personal data in the Cloud? Which Law(s) apply to personal data in the Cloud? How do restrictions on International data transfers work in the Cloud? These issues are addressed briefly below with an analysis of the difficulty in applying the current data protection legal framework to cloud computing.

Personal data in the cloud[34]

The issue of what is considered as personal data in the Cloud is central to the application of data protection laws. The EU Data Protection Directive and the national laws based on it only apply to

* The Commission has set out the working papers on these at <http://ec.europa.eu/justice/data-protection/document/international-transfers/binding-corporate-rules/tools/index_en.htm>

† The list of EU Member State data protection authorities is available on the European Commission website at http://ec.europa.eu/justice/data-protection/bodies/authorities/eu/index_en.htm

‡ So named because it is created under Article 29 of the DPD. http://ec.europa.eu/justice/data-protection/article-29/index_en.htm

'personal data'. The definition of personal data in the EU Data Protection Directive applies to data that is about an identifiable individual. This is a question of fact and may depend on context.[35] That context includes the other information which is potentially available to the data controller, and so whether data is personal data cannot be determined from that data alone. In cloud, this is complicated by whether data should be treated as personal data in various different contexts: anonymized and pseudonymized data in cloud; encrypted data in cloud; and finally sharding or fragmentation of data in cloud. These forms of data involve different processes applied to personal data but in all cases whether the data remains personal data depends on the likelihood of identifying an individual. A 'mere hypothetical possibility' to single out someone is not enough to make the person identifiable.[36] Nevertheless, this area of law lacks clarity. The status of encrypted and anonymized data has not been clarified in the law. The DPD dates from 1995 when technologies relating to anonymization, encryption and pseudonymization were only just developing. Therefore data controllers may need to adopt a cautious approach to personal data and the risks of someone re-identifying individuals from data.

The distinction between data processors and data controllers in cloud[37]

Data protection law is based on regulating the data controllers who are responsible for complying with data protection laws. In data protection law based on the EU Data Protection Directive, the distinction between the data controller and the data processor is key to applying the law. The data controller has the main responsibility to comply with the law, while processors are not normally subject to data protection obligations. The complexity of this area particularly since the development of the Internet has meant that the distinction between the data controller and data processor is not as straightforward as originally hoped.[38] The official position by the Article 29 Working Party is that cloud providers are considered data processors, unless they become data controllers because they act in a manner inconsistent with their instructions.[39] This is not the full picture and does not reflect the reality that the distinctions between data processor and data controller in cloud can be utterly blurred. For example, many cloud providers who run social networking or webmail services run advertisements based on the content of uploaded personal data and so are likely to be data controllers.[40] They are not merely processing uploaded data, but they are accessing it for its own purposes, i.e. targeting advertising to cloud users based on the uploaded data and consequently these cloud providers are data controllers. Examples like this illustrate how artificial is the distinction between data processor and data controller and how one entity can be both in cloud.

The position of sub-providers in the cloud computing chain of responsibility in respect of data protection also complicates matters. Guidance by data protection regulators[41] regarding sub-providers in cloud and the chain of contractual responsibility often reflect a traditional 'outsourcing' view of the contractual relationship between the cloud provider and sub-providers, where the cloud provider delegates processing to its sub-provider. The reality is that many providers with sub-providers have already created services based on the sub-provider's service.[42] Many Cloud services are pre-packaged services built on existing sub-provider services and sub-provider terms and providers may not want, or even be able, to change pre-existing arrangements with sub-providers for every new contract. Therefore this limited degree of control over sub-providers may mean that they are acting as a data controller rather than a data processor. Consequently, the current state of the law with its distinction between data controllers and data processors is less and less satisfactory in cloud.

Deciding which laws apply to personal data in clouds

The issue of the Data Protection Directive applying to cloud computing providers and users outside the EEA and the jurisdiction of data protection authorities to regulate them is one that creates considerable uncertainty for cloud users and providers.[43] Member States' data protection rules are not harmonized and their interpretations of the Data Protection Directive's jurisdictional scope are unclear. The fact that data processing is 'somewhere in the cloud' does not automatically exempt it from the Data Protection Directive. However, identifying when an entity falls within the jurisdiction of EU data protection law requires simplification and clarification of the current law on jurisdiction. One goal of the new proposed Regulation is to clarify applicable law and to improve harmonization in the EU on this point.

Restrictions on international data transfer in cloud

Cloud computing is potentially affected by restrictions on transferring personal data outside the EEA under the Data Protection Directive.[44] Under the Data Protection Directive, subject to certain derogations, Member States must not allow a data controller to transfer personal data to a country outside the EEA, unless the country provides an adequate level of protection under the DPD.[45] We call such transfers 'data export'. Where the third country does not provide an adequate level of protection, the DPD prohibits export of personal data from the EEA unless derogations or special arrangements are made to assure adequacy. The Data Protection Directive when drafted did not fully take into account the complexity of the international data transfers required by the Internet and did not envisage cloud computing at all. Cloud computing by its nature involves data transfers from user to cloud and vice versa and many cloud arrangements use remote data storage and other data processing, so that the data may be replicated to equipment located in third countries.[46] This means that data can be located in a multiple locations at any one time and the result is that the provisions in the Directive and the national laws based on the Directive in the EU restricting data export are neither clear nor sufficiently harmonized across the Member States. This creates even further legal uncertainty about using Cloud.

Cloud and managing the problems with current data protection law

Compliance with the current law is extremely difficult for Cloud providers and users since the law is particularly ambiguous and has not been drafted for an online world, let alone for Cloud. The danger is that the uncertainty could lead to paralysis and fear of uptake of Cloud by some customers, particularly in the public sector.[47] The other potentially negative consequence is that cloud providers will just ignore the law.

The current proposed reform of EU data protection law is not particularly focussed on the Cloud. As they stand,[*] the proposed reforms may help with some matters, for example clarifying the issue of jurisdiction, but may make some issues worse, for example increasing restrictions on international data transfers. One way of managing the problems with current data protection laws and Cloud is by ensuring that the contractual obligations as regards data location and confidentiality as well as provisions on data transfer, security and audit rights are all addressed and well defined.

4.1.2 Trade secrets laws

Although the field of data protection regulation is to some extent harmonised, at least across the European Union, when it comes to protection of business sensitive information and trade secrets, the laws vary. This section offers an overview of the law regarding business sensitive information focusing especially on the breach of contractual obligations, as well as the proposed Trade Secrets Directive.[†]

4.1.2.1 TRIPS Agreement

It is perhaps most useful to begin with the regulatory framework provided by the World Trade Organisation's 1994 TRIPS Agreement (Agreement on Trade-Related Aspects of Intellectual Property Rights). Article 39 focuses on "undisclosed information" and establishes minimum requirements for the protection of such information. Its provisions generally provide that undisclosed information will be protected where:

1. The information is secret (in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among person within the circles that normally deal with such information)
2. There is commercial value because the information is secret
3. Reasonable steps have been taken to maintain the secrecy of the information

[*] The package of reform proposals published by the European Commission on 25 January 2012 are available at http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm

[†] The D4 Work Package is also specifically analysing the remedies and redress mechanisms for business sensitive information and is expected to offer more on that specific aspect of this topic.

As will be seen below, these basic parameters have been adopted by both the civil law and common law jurisdictions through the development of the applicable codes and case law. Also notable is that oftentimes there will be contracts among the party holding the rights to the trade secrets or confidential information.

4.1.2.2 EU framework

At present there is no EU framework for business sensitive information. Nevertheless, most Cloud contracts, especially those negotiated and/or prepared by lawyers, will (and should) include terms and conditions among the various actors regarding the use and non-disclosure of confidential business information being disclosed as a result of the performance of the contract. In the event of a breach of such provisions, the harmed party would then have recourse and remedies through such contractual provisions before the court and which most courts would be prepared to enforce, whether it be through damages and/or injunctive relief.

However, oftentimes the contracts will not address such situations and/or a remedy may be needed against a non-party to a contract who improperly uses or discloses business sensitive information (which is also referred to at times as confidential information and/or trade secrets). Parties harmed by such violations may then have no other remedy but to turn to the law to find a remedy. In that regard, national laws throughout the EU regarding the misappropriation of business sensitive information differ significantly.[48] For instance, some Member States like "Austria, Bulgaria, the Czech Republic, Estonia, Germany, Finland, Greece, Hungary, Italy, Latvia, Lithuania, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden have specific legislation on misappropriation of trade secrets, although some of them fail to define what trade secrets are (examples: Germany, Finland, Greece, Denmark, Spain). In others, like Belgium, France, Ireland, Luxembourg, Malta, the Netherlands, there are no specific provisions on trade secrets in civil law"[49].

Contrary to the Member States referenced above, many common law jurisdictions have developed rights and remedies regarding such breaches. The common law of the United Kingdom is perhaps the best illustrative of how trade secrets and confidential information are protected under common law in the European Union and is well-developed with many illustrative cases and nuances.

In particular, most claims involving acts and/or omissions involving trade secrets fall under the umbrella of a claim for breach of confidence. While this is technically a claim for equitable relief, courts have applied it more like a tort claim. The term 'trade secret' is believed to have first been used in a court decision in *Newberry v. James* (1817) 2 Mer. 446, 35 Eng. Rep. 1011, 1013 (Ct. Ch. 1817). The basis for a claim for breach of confidence thereafter was established in *Morison v. Moat* (1851) 9 Hare 241, per Turner V-C, where it was held:

> In some cases, it [the jurisdiction of the court] has been referred to property, in others to contract, and in others, again, it has been treated as founded upon trust or confidence, meaning, as we conceive, that the court fastens the obligation on the conscience of the party, and enforces it against him in the same manner as it enforces against a party to whom a benefit is given the obligation of performing a promise on the faith of which the benefit has been conferred; but, upon *whatever grounds the jurisdiction is founded, the authorities leave no doubt as to the exercise of it*.

Coco v. A.N. Clark (Engineers) Ltd. [1969] R.P.C. 41 is widely considered the leading modern case on a claim for breach of confidence and provides that three elements must be established to prevail on such a claim:

1. The information must be confidential
2. The information must be disclosed in circumstances giving rise to an obligation of confidence
3. There must be actual or anticipated unauthorized use or disclosure of information

There are some other important requirements in regard to a claim for breach of confidence. First, in order to bring such a claim, the claimant must establish that it is the person to whom the duty of confidence is owed.[50] A duty of confidence arises out of the relationship between two entities, and so it is quite possible that for any piece of information person A would owe the claimant a duty of confidence while person B does not.

Second, there is no need to show any detriment from the breach of confidence when it involved personal or commercial information (diversion of potential business suffices to show damages), though detriment is required to be shown when the confidential information is government information.[51]

Finally, the determination as to whether there has been a breach of confidence will be contextually dependent. For example, in a contract situation, the determination will depend on the contract; in an implied situation it depends on the purpose of why the information was disclosed; and in other cases, an objective test is applied as to the confidant's own conscience, i.e., would a reasonable confidant, under the same circumstances, think that his action amount to a breach of confidence?

English courts have also examined the first two elements in greater detail (with the third element largely speaking for itself and either happening or not happening). As to the first element of whether the information is confidential, in determining whether the information is confidential, courts have held that the information must be sufficiently developed, i.e. the information must be fairly specific, rather than a mere idea, and the kind of information that the relevant industry would deem involved protectable concepts.[52] Courts have also held that the information must be inaccessible or maintained in relative secrecy (absolute secrecy is therefore not necessary for information being deemed as confidential).[53] In further examining this requirement, courts have generally looked to commercial considerations, including whether appropriate security measures have been taken to protect the information such as managing information flows and access, whether and what sort of restrictions have been placed on the use and disclosure of the information (generally through purpose limitations), whether there has been active policing and enforcement of the measures taken in respect to maintaining the confidentiality of the information, and whether there are any non-compete provisions required from those to whom the information is disclosed.

Finally, the information must not already be in the public domain. For example, the information must not be well known to the section of the public that has an interest in knowing the information.[54] However, where confidential information is shown to a limited set of people, e.g. friends, families, and co-venturers – depending on the circumstances, the information will still be deemed to be confidential.[55] But information which has been published, even if it is not easily accessible to the public at large, will have lost its confidential nature.[56]

As to the second element, whether the disclosure gives rise to an obligation of confidence, there are two general categories of such circumstances. The first category is where there is an express obligation imposed on the confidant through an agreement. Such obligations are generally found in non-disclosure agreements or in larger contracts such as outsourcing agreements, data processing contracts, or similar type contracts. In reviewing and applying such contracts, the terms must be reasonable and there remain exceptions where the obligation will not be applied despite the parties' agreement, such as where the information has come into the public domain, a party was in possession of information before agreement was entered, or where the information is acquired from a third party. There is also an exception where the disclosure is justified in the public interest, such as a disclosure of unlawful behaviour by the confider.[57] This defence is not just limited to cases of wrongdoing by the plaintiffs, i.e. the inequality rule; but there are also limitations where someone does not need to disclose to the whole world where lesser disclosure may suffice. And, importantly, these protections have been codified in the UK in the Public Interest Disclosure Act 1998.

The second category is where law implies the obligation. Typical situations where a duty of confidence will be implied by law include where a fiduciary duty exists, e.g., where there is a special relationship between two parties, such as officers or directors of a business entity to its owners, business partners, an attorney-client relationship, etc. Outside such inherently confidential relationships, as the court held in *Coco v. Clark*, a party is bound to respect the confidentiality of information which has been disclosed to him if he either knew or ought in the circumstances to have known that the information was communicated to him in confidence. Examples might include where information is disclosed in a

business-like relationship, with a joint venture in mind, or in relation to the manufacture of articles. An implied duty will often apply in other relationships, such as in the employment context. Courts have even found an implied duty where there was no direct relationship between the parties, imposing the duty on a third party learning of confidential information and knowing it to be confidential.[58] Finally, a duty of confidence has even been extended to strangers where the stranger had knowledge that the information they were disclosing or otherwise using without authorisation was confidential.[59]

There are generally four remedies available for breach of confidence. None of these are exclusive and all will generally be ordered if there has been a breach of confidence. The first is injunctive relief*, where a party can be ordered not to make further use or disclosure of the confidential information. The second remedy is the compulsion of an account for profits, where the offending party will be compelled to account for all uses and disclosure of the confidential information, as well as any monies received as a result of such use and disclosure. The third remedy is the delivery up/destruction of the confidential information, where the offending party will be required to deliver all confidential information to the party owning the information and/or otherwise destroy any remaining copies of the confidential information. Finally, the fourth remedy is monetary damages, which can be determined by the market value of the information, a fair remuneration of what licensing fees would have been, and/or the loss suffered by the claimant (including loss of potential profits) from the unauthorized use or disclosure of the information.

There are three other related concepts worth mentioning in respect to trade secrets. The first is what has come to be known as the springboard doctrine as adopted in *Terrapin Ltd v. Builders' Supply Co (Hayes) Ltd*[60], where that court held that "a person who has obtained information in confidence is not allowed to use it as a springboard for activities detrimental to the person who made the confidential communication, and springboard it remains, even when all the features have been published or can be ascertained by actual inspection by any member of the public." The basis of this concept is that, although the information has now ceased to be confidential, the confidant wrongly used it while it was still confidential. This gives the confidant a commercial lead in the market, and fairness and justice requires that the advantage be taken away. This doctrine has resulted in courts sometimes imposing what are known as "springboard" injunctions to prevent any unfair advantage from a breach of confidence, though such injunctions will not last for an unlimited period of time and only for the period of time where the unfair advantage is expected to last.

4.1.2.3 Proposed Directive on Trade Secrets

On 28 November 2013, the European Commission published a Proposal for a Directive "*on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure*"[61]. The Proposed Directive aims to harmonise national civil law remedies against the misappropriation of trade secrets and rules on preservation of confidentiality of trade secrets during and after legal proceedings.[62] The proposal is in full alignment with the TRIPS Agreement obligations: it will largely align the protection of business sensitive information within the EU with that of the US. The main features of the proposal include:

- the establishment of common principles, definitions and safeguards;
- a limitation period of six years in which to bring an action for civil law redress;
- the preservation of confidentiality during the course of the legal proceedings; and
- a favourable regime for protecting employees in the event of a violation of a trade secret, but where the disclosure was unintentional.

Such harmonised EU rules are ultimately expected to influence a global level of protection of business sensitive information, within the spirit of the TRIPS Agreement discussed above.

* Injunctive relief is an equitable remedy available to courts which empowers them to prevent certain acts or to compel certain acts. Such relief can be preliminary and temporary in nature, for example to preserve the status quo while a case is pending, or can be permanent in nature, whereby courts may prevent certain acts permanently, even after the case before it is otherwise resolved.

In conclusion, most protections for businesses will be provided for by contract. In the absence of such protections, businesses will have no other alternative but to turn to the applicable jurisdiction, hence our initial discussion on the importance, and quagmire, of jurisdiction. In civil law countries, businesses will oftentimes be left without a remedy. In common law jurisdictions, there are generally protections and remedies available through the development of case law and/or through statutes and codes. Finally, the EU is attempting to harmonise the approach in the EU through the proposal of the Trade Secrets Directive in order to establish a common set of definitions, procedures and remedies throughout the EU in regard to trade secrets. It is still uncertain whether that directive will be enacted, but adoption appears likely before the end of 2015.

4.1.3 Consumer protection laws

Although the biggest focus of this deliverable is accountability in respect of data protection laws, it is important not to ignore another large area of law impacting cloud computing, consumer protection. Consumer protection laws are designed to protect consumers both by prohibiting business practices that exploit consumers and by ensuring that consumers have rights of redress. In essence, consumer protection laws are a variety of government regulation governing business-to-consumer contracts that impose obligations on business and that grant rights to consumers. Consumer protection laws may, for example, require a seller to provide additional information to consumers to enable them to make informed choices or it may constrain the terms of contracts with consumers. Specialist organisations, both governmental and private, such as consumer protection bodies or consumer watchdogs, act to defend consumer rights based on these laws.

In examining consumer protection laws, it is important first to understand how a "consumer" is generally defined. Typically, a consumer is considered to be a natural person acting for his or her own personal purposes and not for any business purpose. The consumer is acquiring goods or services for direct use or ownership and is not engaged in resale or use in business. This is important, especially in reviewing consumer protection laws, as the protection afforded by consumer protection laws only apply to consumers and not to businesses.

In examining consumer protection laws, it is useful to divide them into ex ante and ex post consumer protections. As Cunningham and Reed (2013) noted:

> We can separate these consumer protection laws conceptually into ex ante law and ex post laws: those that attempt to create prior to any consumer/supplier relationship an equitable situation, and those that ensure that there is equitable redress for any imbalance that may result from a contractual relationship by, for example, imposing statutory implied terms or rendering unfair terms unenforceable.[63]

In essence this means that ex ante laws aim to make sure that the consumer understands the transaction fully before agreeing to it. In contrast, ex post laws protect from unfair terms which have an adverse impact on the consumer.

As regards the ex ante rights, the consumer protection legislation is mainly concerned with the provision of information to the customer.

- It involves controls on how on marketing is carried out. For example the *Unfair Commercial Practices Directive*[64] prohibits traders from making false or misleading statements about the price or availability of products.[65]

- It may involve provision of information to all customers (both business and consumer customers) as in the *E-Commerce Directive*[66]*.* This applies to providers of 'information society services'[67], a category which includes cloud providers. It requires that such providers need to ensure that specified information is easily, directly and permanently accessible to recipients of the service they provide i.e. that they provide the name of the service provider, their contact details on their website, the details of their trade registration and VAT number.[68]

- It involves requirements that detailed prior information is available to consumers. For example the *Consumer Rights Directive*[69] protects consumers by requiring that detailed pre-contractual information be made available to the consumer about a range of matters that include price, payment, delivery, performance, contract duration, conditions for termination and right of withdraw from the contract.

- In addition the process of signing up to the contract is covered in both the *E-Commerce Directive*[70] and the *Consumer Rights Directive*[71] where there is some overlap to protect the customer.

The most significant EU consumer protection laws are examined below to explain how they would apply to protecting a consumer of cloud computing services in respect of that consumer's personal data and confidential information.

4.1.3.1 Prohibition on Unfair Business to Consumer Commercial Practices

The *Unfair Commercial Practices Directive*[72] prohibits unfair commercial practices pre-contract. The key provisions and how they apply in cloud computing contracts are set out below:

- *Annex I* contains a list of commercial practices which are to be considered unfair in all circumstances and which are therefore prohibited.[73] These are commercial practices that can be deemed to be unfair without a case-by-case assessment since this behaviour is always considered unfair. An example of such a practice is a trader claiming to be a signatory to a code of conduct when the trader is not.

- *Misleading action or omissions* - This relates to misleading actions or omissions, which are those that contain false information and are therefore untruthful or those that, in overall presentation, in any way deceive or are likely to deceive the average consumer in relation to a number of matters listed AND are likely to induce transactional decisions. The matters listed include such things as the nature of the product, the main characteristics of the product and the price. In relation to cloud computing this is relevant in relation to quality of service promises[74], which are crucial to the consumer's decision to trust their information to that cloud provider. It is a common Cloud industry practice to sub-contract or 'layer' facilities amongst and between any number of cloud companies and difficult to communicate succinctly to a potential consumer why this might be a necessary aspect of a service, let alone what its implications are for issues such as who has access to data and how it is safeguarded. In addition, the issue of misleading omissions might have some importance for cloud companies where the cloud service is offered ostensibly for free but still involves complex commercial intentions relating to the provider's use of the consumer's data, which are often not explained explicitly or clearly to the consumer.[75]

- *Aggressive practices* - aggressive commercial practices which cause a consumer to make a transactional decision that he would not have taken otherwise. Although it is not impossible that potential cloud product users will be harassed in order to impair their freedom of choice, this is improbable since there are unlikely to be sales staff for business to consumer cloud services who would engage in the types of selling practices considered aggressive.

- *Unfair commercial practices* - these are practices that cannot be categorised as a misleading action or omission or an aggressive practice but are nevertheless considered unfair. A commercial practice will be considered unfair if it contravenes

the requirements of professional diligence and it materially distorts or is likely to materially distort the economic behaviour of the average consumer with regard to the product. This is a catch-all provision covering the trader's lack of care and skill, contrary to good faith and materially distorting the consumer's economic behaviour. In a cloud computing contract, it might potentially extend to poor security practices not disclosed to the consumer.

- *Sanctions* – these are imposed by public law so they depend on how the Member State implements the directive into national law, but the likelihood is that most Member States will impose fines on the service provider for breach.

4.1.3.2 Obligations to provide detailed information

Obligations to provide information are set out in both the *E-Commerce Directive* and the *Consumer Rights Directive*. The Electronic Commerce Directive obliges any person providing an information society service* to make available to the recipient of the service, in a form and manner which is easily, directly and permanently accessible, certain information which is relevant to trust, performance, payment and redress.†

This requirement to provide information is also supplemented by the *Consumer Rights Directive* in Article 6. Article 6 states that the trader must provide the consumer with a long list of information in a clear and comprehensible manner, and again much of this information is relevant to accountability. The requirements which might have some particular relevancy for cloud computing include: details concerning the arrangements for payment; performance; where applicable, the trader's complaint handling policy; the existence of relevant codes of conduct and how copies of them can be obtained; details concerning the duration of the contract or, if the contract is of indeterminate duration or is to be extended automatically, the conditions for terminating the contract; the conditions relating to the right of withdrawal; details concerning, where applicable, any relevant interoperability of digital content with hardware and software that the trader is aware of or can reasonably be expected to have been aware of; and, where applicable, the possibility of having recourse to an out-of-court complaint and redress mechanism, to which the trader is subject, and the methods for having access to it must be communicated to the consumer.

* Defined as having the meaning in Article 2 (a) of the Directive; the Directive states that information society services are services within the meaning of Article 1(2) of Directive 98/34/EC as amended by Directive 98/48/EC. Directive 98/48/EC, amending Directive 98/34/EC provides a procedure for the provision of information in the field of technical standards and regulations defines services as 'any Information Society service, that is to say, any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services. For the purposes of this definition: 'at a distance' means that the service is provided without the parties being simultaneously present; 'by electronic means' means that the service is sent initially and received at its destination by means of electronic equipment for the processing (including digital compression) and storage of data, and entirely transmitted, conveyed and received by wire, by radio, by optical means or by other electromagnetic means; 'at the individual request of a recipient of services' means that the service is provided through the transmission of data on individual request.

† Article 5. This includes the name of the service provider; the geographic address at which the service provider is established; the details of the service provider, including his electronic mail address; details of any trade register in which the service provider is registered and his registration number of equivalent means of identification; the particulars of any relevant supervisory authority which the service provider is subject to; where the service provider 'exercises a regulated profession' the details of any relevant professional body with which the service provider is registered, the professional title of the service provider and the member state where that title was granted and a reference to the professional rules applicable to the service provider and the means of access to them; and, where the service provider undertakes an activity subject to value added tax, the relevant identification number.

4.1.3.3 Right to consumers to withdraw from contracts

The *Consumer Rights Directive* gives consumers a right to withdraw from a contract.[76] The period for consumers to withdraw from any distance purchase is 14 days, and business to consumer (B2C) cloud computing services are universally sold online and therefore at a distance. The consumer can change their mind and cancel the contract without the need to give any reasons within that period. The 14-day period is calculated from the date when the contract for services is made. If the provider has not clearly informed the consumer about the right to cancel the contract, the period is extended to a year. Traders must reimburse the consumer within 14 days of cancellation, though the consumer must pay for any services which have already been received.

Article 16 lists several situations in which the consumer has no right of withdraw or loses his right of withdrawal under certain circumstances. The most relevant to cloud computing are contracts where the services have been fully performed (though this is unlikely in the cloud context, as most contracts are for continuing use of a service) or contracts for the supply of digital content where the supply has already begun. In both cases, the exception only applies if the consumer has been informed of the right of withdrawal, has expressly consented to the supply beginning and has acknowledged (most likely by ticking a box on screen) that the right of withdrawal will be lost.

4.1.3.4 Rights for consumers during the contracting process

The *Electronic Commerce Directive* provides consumers with rights prior to concluding a contract and while concluding a contract. Article 10 provides that prior to an order being placed by the recipient of a service, the service provider must provide in a clear, comprehensible and unambiguous manner: the different technical steps to follow to conclude the contract; whether or not the concluded contract will be filed by the service provider and whether it will be accessible; the technical means for identifying and correcting errors prior to the placing of the order; and the languages offered for the conclusion of the contract. In addition, under Article 5 price references must be indicated clearly and unambiguously and shall indicate whether they are inclusive of tax such as value added tax and delivery costs.

To protect consumers against the consequences of making errors when they sign up to a service, Article 11 of the Directive provides that where the recipient of a service places his order through technological means, the service provider must – unless parties who are not consumers have agreed otherwise – acknowledge receipt of the order without undue delay and by electronic means, and also make available to the recipient of the service appropriate, effective and accessible technical means allowing him to identify and correct input errors prior to the placing of the order.

4.1.3.5 Ex-post rights for consumers under the Unfair Contract Terms Directive

The Unfair Contract Terms Directive[77] deals with the ex-post situation where the consumer has already entered into a contract, but now seeks redress against the service provider. Such a claim for redress will most likely be for breach of contract by the provider, and therefore under contract law it is, at first instance, determined by reference to the terms of the contract. Even if the claim is a non-contractual one, eg a claim under data protection law for loss caused by unauthorised disclosure, or a claim in negligence for data loss, the terms of the contract may attempt to prevent or limit the making of such a claim. B2C cloud computing contracts are always on standard terms, drafted by the cloud provider, and this is likely to bias them in favour of the provider.

The Directive applies to unfair terms in contracts concluded between a seller or a supplier and a consumer that have not been individually negotiated, and provides that those terms are unenforceable against the consumer, although the remaining terms continue to bind both parties.[78] This means that it applies to standard contractual terms imposed on consumers.

Contract terms are regarded as unfair if, contrary to the requirement of good faith, they cause a significant imbalance in the parties' rights and obligations arising under the contract, to the detriment of the consumer. The Directive contains an annex of indicative terms which are likely to be unfair – for

example, excluding or hindering the consumer's right to take legal action or exercise any other legal remedy, particularly by requiring the consumer to take disputes exclusively to arbitration; and irrevocably binding the consumer to terms with which he had no real opportunity of becoming acquainted before the conclusion of the contract.

B2C cloud contracts are full of terms which are potentially unfair. The most obvious is exclusion or limitation of liability. This is not automatically unfair, if only because of the disproportionate liability risk that a cloud provider would carry in proportion to its income from the consumer service, but a blanket and unjustified total exclusion will almost certainly be unfair. Limiting access to the courts is common practice in US consumer contracts, which often impose exclusive arbitration clauses, primarily to avoid the risk of jury trials and the award of damages which go beyond pure compensation[*], and this drafting often finds its way into cloud contracts with EU consumers. It is also common to provide that terms may be changed simply by posting a notice on the provider's website, and arguably this gives the consumer no real opportunity of discovering the change.

It is also worth noting that privacy policies normally form part of the B2C contract and thus their provisions can be challenged under the Directive. The starting point for fairness is explaining the policy clearly and accurately, rather than relying on vague descriptions such as data sharing with unidentifiable "affiliates". But, given that it is notorious that consumers do not read the terms to which they sign up, and that a substantial proportion of privacy policies are too difficult for the average consumer to understand[79], it is likely that full disclosure is insufficient to achieve fairness.

These matters have yet to be tested in court, but it is important to note that the Directive adds a further layer of uncertainty to the law which is relevant to accountability. Contracts, if properly drafted, can make very clear statements about the rights and liabilities of the parties, but a B2C contract may not mean what it appears to say if some of its terms are unfair and thus unenforceable.

4.1.4 Miscellaneous laws

Behind the Data Protection Directive, the second most important European law impacting the Cloud is Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (e-Privacy Directive). Article 1 of the e-Privacy Directive provides its underlying goal:

> This Directive harmonises the provisions of the Member States required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy, with respect to the processing of personal data in the electronic communication sector and to ensure the free movement of such data and of electronic communication equipment and services in the Community.

As seen by Article 1, the e-Privacy Directive applies to 'the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks' in the EU. Critically, the Directive does not apply unless the electronic communications service is publicly available. This means that communications over a private network, e.g., a company intranet, are not governed by the e-Privacy Directive, but the Data Protection Directive would still apply.

The key provisions of the e-Privacy Directive, at least in respect to the Cloud and Cloud Providers and users, include:

- Providers are required to take appropriate technical and organisational measures to safeguard the security of the services being offered.

[*] These are termed exemplary and punitive damages, and are imposed to mark the court's disapproval of the defendant's conduct, or to deter such conduct in the future and deprive the defendant of the likely profits from past conduct.

- Providers are under a general obligation to inform a subscriber of any particular risk of breach of the network's security.

- Member States are required to maintain the confidentiality of communications and of the associated traffic data generated by such communications, subject to specific exceptions, including where interception and surveillance is otherwise authorised by law.

- Location data may be processed only if that data is made anonymous, or if not, if done with the consent of the user and for the duration necessary for the provision of a value-added service.

- The mandatory notification by electronic communications service providers of any personal data breaches to both the relevant national authority and the relevant individual in cases where the breach is likely to "adversely affect the personal data or privacy of a subscriber or individual.'

- Allowing the storing of or the accessing of previously stored personal information, i.e. cookies, in the terminal equipment of a subscriber or user only when the user has given his or her consent after having been provided with a clear and comprehensive statement regarding the storage in compliance with the Data Protection Directive. There are two exceptions: (1) where the storage is for the sole purpose of carrying out the transmission of a communication over an electronic communication networks; or (2) where the storage is strictly necessary for the provision of an information society service explicitly requested by the subscriber or user.

The other important European directive impacting the Cloud is Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks (Data Retention Directive). This Directive aims to harmonise the rules on data retention across the EU for serious crime and antiterrorism purposes. Critically, the provisions of the Data Retention Directive do not apply to content of any data, only information concerning the traffic data, location data and enough data to identify the subscriber and/or registered user.* While 'providers of publicly available electronic communications services' or 'public communications networks' are not defined in the Data Retention Directive, it generally has been applied to email, Internet access, fixed network telephony, mobile telephony, and Internet telephony. Thus, information generally required to be maintained, depending on the method of communication, includes the incoming and outgoing telephone numbers, name and address details of the subscribers, IP addresses, date and time of the start and end of telephone calls, date and time of log-in and log-off of Internet access and e-mail systems. When a competent national authority requests such information, it must be turned over without undue delay. Finally, the length of time that such information must be retained has been left to the Member States, though the Data Protection Directive mandates the period of time to be no less than six months and no more than two years from the date of the communication. The data must be erased after the expiration of the two-year period.†

* The Data Retention Directive does not prohibit the retention of data, though, as discussed above, the Data Protection Directive and/or proposed Data Protection Regulation would likely still apply in most situations and require purpose and/or consent for any continued storage of personal data beyond the initial purpose for collection and storage.

† Notably, there has been quite a bit of backlash against the Data Protection Directive based on arguments that it violates personal privacy. Germany's highest court has ruled that Germany's implementation of the Directive was unconstitutional, and therefore null and void, and other Member States, including Ireland and Slovakia, have called for it to be repealed. Thus, many questions regarding the applicability of the Data Retention Directive remain and there will likely be ongoing challenges to its scope, applicability and other requirements.

4.2 U.S. laws

The U.S. takes a far less than paternal approach than the EU when it comes to consumer protection. Nevertheless, many of the basic principles, underlying legislation and, more importantly, enforcement, tend to overlap. And, as noted above in respect to jurisdiction and as seen in greater detail below, the U.S. has a plethora of laws between its federal and state laws, as well as the various courts interpreting and applying such laws. This again highlights the maze of regulations of Cloud Providers must navigate.

4.2.1 Data protection and privacy laws

Quite different from the comprehensive approach to data protection undertaken by the EU, the U.S. instead largely follows a sectoral model. This means that the U.S. has only provided for specific protections in certain industries, though, as seen below, the U.S. has expanded general protections provided to consumers and increased scrutiny on businesses in respect to privacy policies and information security. Such areas include the healthcare sector with protection of health records, law enforcement records, consumer financial transactions, telecommunications sectors, the protection of children, and some other narrow fields. Notably, the U.S. does not have an overriding privacy or data protection law, though some of the Amendments to the U.S. Constitution do touch upon privacy rights, including without limitation, the First Amendment (privacy of beliefs and association), the Third Amendment (privacy of the home), and the Fourth Amendment (privacy of the person, communications and the home). Other Amendments, including the Fifth Amendment and Fourteenth Amendment have been cited by U.S. Courts in protecting 'private matters', including the child-rearing, educational choices, procreation, marriage, termination of medical treatment and consenting adult sexuality in the home.

The U.S., generally through the Courts and administrative actions, has also provided greater general protection for citizens' personal information, though such measures and protections have come nowhere close to the codification found in the EU through the Data Protection Directive. And, while the U.S. has not adopted a controlling privacy act as between citizens and/or companies, it has adopted the Privacy Act of 1974 in respect to federal agencies and which provides protections related to the creation, maintenance, use and dissemination of records containing personal information.

Instead, for private protections at the federal level, the Federal Trade Commission, an administrative agency generally empowered to protect trade and consumer issues in the U.S., has the general authority to enforce against "unfair and deceptive trade practices." And, while it has been debated whether that phrase includes data protection and/or privacy rights, the Federal Trade Commission (FTC) has become increasingly proactive since the late nineties in protecting consumers when it comes to data protection, especially in the areas of information security, the collection and processing of data, misleading or unclear privacy notices, and the reselling of data. The overriding principle of law involved is that businesses should not provide misleading information to their customers in respect of data privacy matters.

Some of the most important actions taken by the FTC in this area illustrate its approach to the issue:

- *In the Matter of GeoCities, Inc.*[80] – this represented the first FTC Internet privacy enforcement action in which the FTC alleged that GeoCities, which operated a website promoting an online community on which users could maintain personal home pages, misrepresented how it would use personal information in its privacy notice and also maintained children's personal information without parental consent. GeoCities settled the action and the FTC issued a consent decree.[*]

- *In the Matter of Eli Lilly & Co.*[81] – Eli Lilly & Co. is a pharmaceutical manufacturer which collected personal information from subscribers on its website, including sending

[*] A consent decree is a judgment entered by consent of the parties in which the defendant agrees to cease and desist from the alleged illegal activity, usually without admitting any wrongdoing. *Black's Law Dictionary*, 9th ed., 2009, s.v. "consent decree."

updates to remind customers to take their medicine. When Eli Lilly & Co. ended that program, it inadvertently sent a mass email revealing the email addresses of all subscribers. Eli Lilly & Co. settled the enforcement action brought by the FTC, in which Eli Lilly & Co. agreed to adhere to its representations regarding the collection, use and protection of customer's data. Most notably, this also marked the first case where a defendant was also required to develop and maintain an information privacy and security program.

- *In the Matter of Gateway Learning Corp.*[82] – Gateway Learning maintained a privacy notice stating that it would not sell, rent or loan any customer's personal information without express consent of the customer. The notice also contained an opt-out provision if Gateway Learning's policy changed. Thereafter, Gateway Learning rented out customers' personal information to third-party marketers and advertisers, without providing the opt-out option to the customers. The 2004 consent decree entered against Gateway Learning provided that Gateway Learning would comply with its policy and required Gateway to relinquish all funds obtained from renting its consumers' information.

- *In the Matter of Google Inc.*[83] – this 2011 action resulted from Google's introduction of Google Buzz, a social networking service, which was integrated with Gmail, Google's email service. Gmail users were automatically enrolled in Buzz without having to provide any consent. Buzz utilized information pulled from Gmail, making such information public without disclosing such use to its customers. Such conduct conflicted with Google's own privacy notice contained on its website. The FTC alleged such conduct constituted a deceptive trade practice and that Google was in violation of the US-EU Safe Harbor framework. The consent decree was important for two reasons: (1) it represented the first time there was significant enforcement of the US-EU Safe Harbor by the FTC; and (2) it required Google to implement a comprehensive privacy program, with Google undergoing third-party privacy audits on a biannual basis.

- *In the Matter of Facebook Inc.*[84] – in 2011, Facebook settled this FTC action in which there were eight counts brought against Facebook, mostly arising from Facebook's repeated changes to its services resulting in private information being made public. Pursuant to the consent decree, Facebook was required to (1) provide users with clear notice; (2) obtain user consent before making retroactive changes to privacy terms; (3) refrain from making any further deceptive privacy claims; (4) establish and maintain a comprehensive privacy program; and (5) obtain biannual independent third-party audits of its privacy program for the next twenty years.

- *FTC v. Wyndham Worldwide Corporation, et al.*[85] – this action was brought in the U.S. District Court, District of New Jersey in which the FTC alleged Wyndham Worldwide Corporation, which operated hotels, failed to maintain reasonable and appropriate data security for consumers'' sensitive personal information. Wyndham moved to dismiss the case, but in April of 2014 and in a 42-page opinion, the District Court held that the FTC did have the authority to bring the claims against Wyndham, thereby bolstering the FTC's right to bring privacy and data protection actions and implying security and privacy requirements for businesses that were not otherwise expressly required under law. The case remains pending and it appears likely that Wyndham will appeal the District Court's decision.

Similarly, the Obama Administration has also been more proactive in promulgating overriding principles for data protection, including, individual control, transparency, respect for context, security, access and accuracy, focused collection, and accountability in its 2012 issuance of the report "Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy."[86] In response to that report, the Federal Trade Commission issued a report titled "Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers"[87] guiding companies to follow three general principles of (1) privacy by design; (2) simplified consumer choice; and (3) transparency. In examining those principles, it can be seen that

perhaps the U.S. and EU are not as far apart as to data protection as it would otherwise appear in media reports and other descriptions of the two policies.

4.2.2 Consumer protection laws

Unlike the EU, the U.S. is rather laissez-faire when it comes to consumer protection laws, instead allowing most consumer-oriented industries and businesses to govern themselves, within reason, and for markets to self-correct and regulate through capitalism. As noted below, there are many sectors of industry which are regulated to a greater degree, but largely consumers must fend for themselves, especially in respect to federal laws. Consumers are generally left to do so through civil litigation, though such a course of action largely remains unattractive based on time, cost and complexity. Consumers are oftentimes also protected by FTC actions, based on the same principles detailed above in regard to breached privacy notices and insufficient information security measures, but on a more general basis where there have been unfair or deceptive trade practices. Similar protections are also found in all states and prosecuted through State Attorney Generals. There are also many state agencies that govern specific industries and which may impact businesses conducting business in those states over the Internet or through the Cloud. Finally, there is a fair amount of self-regulation. One such area impacting the Cloud is the Payment Card Institute Data Security Standard (PCI DSS) which provides a security standard for payment card data. PCI DSS requires, with some exceptions for smaller companies, for the hiring of a third party to conduct security assessments and detect violations. Non-compliance can lead companies from being excluded from processing payments through major credit card systems, as well as penalties of up to $100,000 per month.

4.2.3 Trade secret laws

It is important to briefly discuss trade secret protection in the U.S. since many cloud computing contracts among cloud actors contain forum selection provisions choosing courts in the U.S. as the only venue in which to litigate any disputes arising from the contract and/or choice of law provisions providing the law of a certain state, oftentimes California, as the governing law.[88] However, the state of the law regarding trade secrets and the wrongful disclosure or use of sensitive business information in U.S. proves to be a more difficult study in light of its federal laws, state laws, and the development of case law, all of which can vary across those the federal circuit courts and the fifty states. Nevertheless, there are some common features to generalize the typical approach to how trade secrets are approached.

First and foremost, in 1979, the Uniform Law Commission, National Conference of Commissioners on U.S. Laws* proposed a uniform law on trade secrets known as the Uniform Trade Secrets Act. With the exception of New York and Texas, which still rely on common law, all other states have adopted the act.[89] For our purposes, and because many cloud computing contracts are governed by California law, our examination will be of the Uniform Trade Secrets Act as enacted in that state in its Civil Codes Sections 3426 through 3426.11, inclusive.

> Under the Uniform Trade Secrets Act, a trade secret is defined as:
>
> Information, including, without limitation, a formula, pattern, compilation, program, device, method, technique, product, system, process, design, prototype, procedure, computer programming instruction or code that:
>
> (a) Derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by the public or any other persons who can obtain commercial or economic value from its disclosure or use; and
>
> (b) Is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

* This organisation is not empowered to make laws, but rather regularly meets to discuss the harmonisation of laws across the U.S. and proposes uniform laws to be adopted. States are not required to adopt such laws, but normally do so, oftentimes with slight changes from the proposed language by the Uniform Law Commission.

The California Civil Code, § 3426.1(d) further provides:

> "Misappropriation" means:
>
> (1) Acquisition of a trade secret of another by a person who knows or has reason to know that the trade secret was acquired by improper means; or
> (2) Disclosure or use of a trade secret of another without express or implied consent by a person who:
> (A) Used improper means to acquire knowledge of the trade secret; or
> (B) At the time of disclosure or use, knew or had reason to know that his or her knowledge of the trade secret was:
> (i) Derived from or through a person who had utilized improper means to acquire it;
> (ii) Acquired under circumstances giving rise to a duty to maintain its secrecy or limit its use; or
> (iii) Derived from or through a person who owed a duty to the person seeking relief to maintain its secrecy or limit its use; or
> (C) Before a material change of his or her position, knew or had reason to know that it was a trade secret and that knowledge of it had been acquired by accident or mistake.

Ultimately, the Uniform Trade Secrets Act provide remedies similar to those provided in the United Kingdom, including injunctive relief, damages, and licensing fees. California Civil Code, § 3426.2 and 3426.3. Perhaps the biggest difference between UK and U.S. law is that the Uniform Trade Secrets Act provides for an award of exemplary damages not exceeding two times the amount of compensatory damages awarded, but only if there has been wilful and malicious misappropriation. See California Civil Code, § 3426.3(c).

Finally, and notably, the Uniform Trade Secrets Act specifically provides that it does not supersede any contractual remedies agreed to between the parties, other civil remedies available to a party, or any criminal remedies that may also exist. See California Civil Code, § 3426.7(b).

4.2.4 Notable state laws

As referenced above, the U.S. has enacted laws at the federal level, but the fifty states have also enacted their own laws applicable within those states. While those laws often mirror each other, sometimes states have regulated more than the federal laws, thus making it important to examine some of the more notable of those laws which may apply to those businesses conducting business in those jurisdictions.

First and foremost, most of the fifty states have some sort of data breach notification laws and many others have some sort of privacy protections in place. Representative examples of these state laws include:

- **California Online Privacy Protection Act of 2003** – this law requires operator of commercial web sites, or which provide online services, and which collect personal information to conspicuously post a privacy policy and comply with that policy. The privacy policy must contain certain provisions, including without limitation, the categories of personally identifiable information collected from visitors, the categories of third parties with which the information may be shared, and any information about the operator's online tracking practices.[90]

- **California Computer Spyware** – this law prohibits an unauthorized person or entity from knowingly installing or providing software that performs certain functions, including

taking control of a computer or collecting personally identifiable information on a user's computer located in California.[91]

- **Massachusetts Standards for the Protection of Personal Information** – this code requires that any company that possesses personal information must maintain a comprehensive information security program and which contains administrative, technical and physical safeguards which are appropriate to the size and scope of the business; the amount of resources available to the company; the amount of stored data; and the need for security and confidentiality of consumer and employee information. This code further requires that a company designate an employee and/or employees to maintain the program, to conduct a risk assessment, to train employees about such procedures, and to impose disciplinary procedures for violations of the program. Finally, the code generally requires that companies take similar precautions in outsourcing any services involving personal information and to ensure that any contracted third parties maintain similar procedures.[92]

- **Washington State Data Privacy, Breach and Encryption Law** – this law basically provides that residents of Washington must be informed of any personal information breaches. It defines personal information as an "individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted." Critically, the code allows for a company to encrypt personal information, and if a company does so, the code provides a safe harbor from the code. A breach is defined as any unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business." The code allows for civil actions for any breaches of the code, including damages and/or injunctive relief.[93]

Finally, at least 31 states now have some form of laws which require companies (and some have laws that apply to governmental agencies) to destroy, dispose or otherwise make information unreadable or undecipherable when the company no longer is using the information for the purpose it was collected and/or there is no other legitimate purpose under the law for the information to be stored. For example, the State of Michigan has enacted the Identity Theft Protection Act, which provides, in relevant part:

> (1) Subject to subsection (3), a person or agency that maintains a database that includes personal information regarding multiple individuals shall destroy any data that contain personal information concerning an individual when that data is removed from the database and the person or agency is not retaining the data elsewhere for another purpose not prohibited by state or federal law. This subsection does not prohibit a person or agency from retaining data that contain personal information for purposes of an investigation, audit, or internal review.
>
> (2) A person who knowingly violates this section is guilty of a misdemeanor punishable by a fine of not more than $250.00 for each violation. This subsection does not affect the availability of any civil remedy for a violation of state or federal law.
>
> (3) A person or agency is considered to be in compliance with this section if the person or agency is subject to federal law concerning the disposal of records containing personal identifying information and the person or agency is in compliance with that federal law.
>
> (4) As used in this section, "destroy" means to destroy or arrange for the destruction of data by shredding, erasing, or otherwise modifying the data so that they cannot be read, deciphered, or reconstructed through generally available means.

It can be expected that with the increased usage of the Internet, Cloud computing, and other electronic technologies that other states will adopt similar laws and states will continue to evaluate their current laws in determining whether any further protections are necessary. Further compelling such protections

are the increasing number of huge data breaches, especially those involving credit and debit cards and the impact it has had on tens of millions of people's financial information, albeit in varying degrees, being compromised in such breaches.

5 Cloud computing contracts

The other important legal consideration involved in the use of cloud, and a critical method to dealing with legal risks, including the data protection risks, is to manage this by agreeing appropriate safeguards in the contract with the cloud provider. Contract law concerns the legal relationship between individuals, which includes organisations. It applies irrespective of technology and there are no specific standard terms for 'cloud contracts'. This is in contrast to, for example, the law on sale of goods, where the law provides a set of default terms which require specific agreement to depart from (and which consumer law may not permit to be modified, see section 4.1.3 above). A contract for cloud services is normally drafted by the cloud provider, and establishes the 'rules' between the parties and covers who does what, who pays what, what each side expects and is a feature of private law, rather than public regulatory law. We refer to this contract between the end-customer and the cloud provider as the 'cloud contract'.

Contracts can be divided into two categories: the negotiated contracts and the non-negotiated standard-form contracts. Most cloud contracts are non-negotiable standard-form contracts.[94] Because there are forthcoming papers dedicated to the issues of cloud contracts, we not spend a great deal of time herein in addressing such provisions and implications. Nevertheless, it is important to examine the main features of both standard and negotiated contracts. Additionally, we also examine some of the specificities of outsourcing contracts.

5.1 Standard Cloud contracts

Standard terms and conditions are often a feature of contracts between business providers and consumers or small and medium sized enterprise (SME) customers. These customers do not have the bargaining power of larger business customers to negotiate contract terms, nor do they have legal teams to help them negotiate, nor sometimes the interest in negotiating contract terms. Most cloud contracts contain the providers' standard terms designed for high-volume, low-cost, standard services. Many consumer customers click to accept without even reading them.

In a survey of standard cloud contract terms,[95] the results showed that many cloud providers included wide-ranging disclaimers of liability or warranty that the cloud service would operate as described and it included often included remedies only in the form of credits against future services. On the other hand, the research findings showed that there was a range of potential variations between cloud providers in their standard contracts when it concerned matters such as: the threshold for disclosing customer data to third parties, the extent to which data would be maintained by the provider at the end of the contract term and the jurisdiction and choice of law in the contract for contract enforcement.[96] These terms could be significant and influence the choice of cloud provider.

Many consumer and SME customers did not have the know-how to assess the differences between standard cloud contracts. They often clicked their consent to these terms and conditions, without considering whether the standard contract suited them or not.

In the context of accountability, what is required is for providers to assist customers in understanding the effect of the standard cloud contract, and thus how responsibilities for personal data and confidential information are allocated between them, before becoming contractually committed. Given that customers neither read nor understand legal terms, this is not a task in which lawyers can assist. Alternative approaches are badly needed, such as the development of the COAT tool under work package D4 which aims, in relevant part, to briefly explain legal provisions of terms and conditions to consumers and to assist them with matching their needs with services provided by Cloud providers.[*]

[*] A more detailed analysis of how that tool will assist in increasing accountability in legal and regulatory terms will be carried out in Deliverable D44.6.

5.2 Negotiated Cloud Contracts

Negotiated contracts for cloud services are the exception rather than the rule and are often confined to large corporate customers.[97] Contract negotiation often depends on the economic bargaining power between the respective parties and cloud contracts are no different. The starting point for cloud contracts is usually the providers' standard terms and, since these do not accommodate large business users' needs, cloud users seek to negotiate.[98]

The decision to negotiate may be driven by internal commercial issues or external issues.[99] For example, the customer may require higher service levels for certain critical services. The decision may also depend on the need to comply with regulatory requirements and laws. A review of the main terms that cloud customers seek to negotiate[100] include the following clauses:

- *limitation of liability clauses*[101] – Cloud providers' terms that limited or entirely excluded liability for data loss or for service outages were, unsurprisingly, the most important terms that cloud customers wanted to negotiate. It was also an area where cloud providers were most like to be intransigent, excluding or capping liability. The nature of the service was a factor in negotiations, with providers more reluctant to accept liability for cheap, commoditized services than for bespoke services. The type of customer also played a role; governments and financial institutions, for example, would insist on unlimited provider liability for certain types of loss caused by breach of regulation or security requirements.

- *clauses concerning data integrity and business continuity* – Cloud providers tend to provide backup as a separate services, so that if the user pays extra, the provider will make backups. Back-up service does not mean, however, that providers will warrant data integrity or accept liability for data loss and therefore additional specific warranties need to be negotiated with providers.[102]

- *service levels* – The approach to service level agreements (SLAs) covering matters such as availability levels and performance often led to debate between customers concerning methods for measuring service levels.[103] As standards in this area develop,[104] agreeing on the key performance indicators (KPIs) will become much easier.

- *regulatory issues*[105] – Clauses mainly relating to the cloud customer needing to demonstrate compliance obligations to regulators since these are often not taken into account in standard cloud contract terms. For example, cloud customers have obtained warranties from cloud providers that all data centres used for their data were in the EU or EEA so that data is kept within the EU and in this way can show data protection authorities that data are not being transferred outside the EEA.

- *confidentiality clauses*[106] – Users want to guarantee the confidentiality of their information, whether it is personal information of an individual user or business data which could even constitute a trade secret.

- *security requirements*[107] – Security requirements are a key user concern. Users may want to specify detailed security requirements, but also ask for audit rights. Some users, particularly in the regulated financial services sector, need audit rights to show to financial auditors and regulators that they are compliant with regulation. In addition users often want security breach notifications from cloud providers, which are often not part of any standard contract terms but are required by large customers.

- *lock-in and exit*[108] – End of contract transition and exit strategy are important to cloud users and concerns about 'lock-in' are often cited as the highest user concerns, after security. Lock-in can mean various concerns but the biggest is the inability to exit a contract and, in a cloud context, the inability to retrieve data from your cloud provider, which could effectively prevent the customer switching from the cloud provider and result in them being "lock-in" to a particular cloud provider. Users want to be able to retrieve data from cloud providers at the end of the contract, or whenever they terminate the contracts. Data portability and data retention on termination of the contract, to allow the customer enough time to retrieve contract data, are key issues in negotiated contracts.

- *term and termination* – The length of the contract and how the contract is terminated, whether by the passage of term, fulfilment of obligations, and/or some other event, i.e. default.

The level of success in negotiating these issues appears to depend on the bargaining power of the customer and their insistence. Large providers generally refuse to negotiate terms and decline changes to their standard terms insisting on a 'take it or leave it' approach even when a large customer requests it.[109] Negotiated cloud contracts are as a result rare and the majority of cloud contracts are on cloud providers' standard terms.

5.3 Outsourcing Contracts

Attention must also be paid to outsourcing. Oftentimes, a Cloud Provider or SME will outsource part or all of its IT functions, thus placing their Cloud Computing functions and/or use outside of its organisational structure. Even more so, the relationships are not as simple as one data controller and one data processor, with there often being long chains which may include multiple data controllers and data processors. One corporate entity may utilise subsidiaries and affiliates to carry out its IT procurement, which then may contract with a broker or another provider which then utilises a number of other entities, sometimes affiliated with the provider, but more often acting independently, to carry out the processing. Critically, in that long chain, an entity which was contracted or subcontracted with as a data processor, may take an active role in the decision-making, which is not surprising as a broker or prime provider will generally have more expertise in regard to data processing. And that is perhaps the most important factor to remember in regard to outsourcing – a data processor that goes beyond its mandate and maintains a relevant role in determining the purposes or essential means of processing will be treated as a data controller. The Article 29 Working Party confirmed the same in its Working Party Opinion WP 169. Equally important, the fact that certain duties and responsibilities are delegated to another entity will not prevent a regulator from enforcing the Data Protection Directive against the responsible party *as defined under the DPD*.

Thus, outsourcing does not alleviate the customer, acting as a data controller under the Data Protection Directive, or the Cloud Provider, also acting as a Data Controller and/or Data Processor under the Data Protection Directive from complying with its legal obligations. For example, Germany, which experienced a number of serious data protection breaches over the past two decades, has taken a much more strict approach in adopting additional requirements in its implementation of the Data Protection Directive known as Bundesdatenschutzgesetz (the "BDSG"). Section 11 of that legislation set forth ten requirements which must be addressed in any processing or outsourcing agreement:

1. The subject and duration of the work to be carried out.
2. The extent, type and purpose of the intended collection, processing or use of the data, the type of data and category of data subjects.
3. The technical and organisational measures to be taken under section 9.
4. The rectification, erasure and blocking of data
5. The processor's obligations under subsection 4, particularly monitoring
6. Any right to issue subcontracts
7. The controller's rights to monitor and the processor's corresponding obligations to cooperate with the controller
8. Violations by the processor or its employees of provisions to protect personal data or of the terms specified by the controller that are subject to the obligation to notify
9. The extent of the controller's authority to issue instructions to the processor
10. The return of data storage media and the erasure of data recorded by the processor after the work has been carried out

Notably, a breach of section 11 is treated as a regulatory offence which carries the imposition of fines of up to €50,000, plus a potential deduction of profits which a party may have received as a result of the breach. Thus, where German law applies, such provisions must be followed. Additionally, many such requirements are already implied by the Data Protection Directive and/or are good practices already.

Moreover, there are other steps the outsourcing entity can take to protect itself vis-à-vis the outsourcing contract:

1. *Establishing and defining roles in the contract* – For the first level of protection, any outsourcing contract should clearly define the parties' roles, i.e. who is the data controller and who is the data processor. As seen above, the Data Protection Directive requires this anyway, but it practically provides protection to all parties in proceeding in their defined roles.

2. *Employment screening* –Security breaches are often caused by the negligence of employees of not performing their job duties responsibly, taking secured data and then losing or having such information stolen, and/or employees which intentionally breach security measures and/or aid others in doing so. Requiring heightened employee vetting and monitoring can greatly assist in minimising such risks.

3. *Disallowing subcontracting and/or requiring equal compliance* –Data processors will often subcontract out some or all of the processing responsibilities to subcontracting data processors. The outsourcing contract should be unambiguous as to whether such subcontracting is allowed. If allowed, then the outsourcing contract should make clear that the same requirements apply, notice of any subcontractors should be required, all subcontractors must meet the same the same standards required of the contracting processor, and ultimately, the contracting supplier must remain liable for any breaches, including any breaches by any subcontractors.

4. *Prompt reporting* – Many data breaches are exacerbated by the lack of prompt reporting, thereby allowing data breaches to continue and/or not allow the processor or controller to take proper remedial measures to minimise the impact of the breach. Therefore, the outsourcing contract should provide for prompt reporting to the outsourcing company.

5. *Indemnification and insurance* – Perhaps most importantly for the protection of the data controller, its customers, and/or consumers exposed to data breaches, the data processor should provide full indemnification for any breaches caused by its own or its employees negligence or intentional acts. Additionally, many major insurance companies are now providing insurance coverage for data breaches and such insurance should be obtained and/or required of the contracting processor and/or any subcontracting processors.

Those rather simple, yet important contractual provisions can provide extra layers of protection and help minimise risk and exposure to data breaches.

6 Redress and remediation

The concept of redress and remediation is to put the person who has suffered harm back in the position that they were in prior to when the harm occurred. This may mean giving a legal remedy to the person. It may also involve having a company policy about how to deal with complaints and how to give the customer redress.

Redress and remediation can consist of a range of different measures. From a purely legal or regulatory perspective, it mainly concerns legal remedies, sanctions, fines, and forms of injunctive relief, i.e. compelling or restraining some type of behaviour. From a business perspective, it may also include how to address a customer's complaints in a way that makes amends for a breach of a customer's rights and that restores their confidence in the company. All means of redress and remediation are covered in this section but the focus is on redress and remediation from the perspective of accountability in A4 Cloud. By this, we mean a cloud provider accounting to the cloud customer, and, ultimately, a cloud customer accounting to its own customers and/or consumers.

Civil legal remedies

A legal remedy is a means by which a court of law enforces a right or imposes a penalty. Legal remedies for redress and remediation may involve enforcement by a public body, like a data protection regulator, or it may concern a dispute under private law for example, one party seeking a remedy for breach of the cloud contract or service level agreement.

Types of civil legal remedy available

There are traditionally three main remedies in civil law for someone that has suffered harm. The first remedy is damages meaning a payment to the victim to compensate an injured victim for the harm suffered. This is the most common type of remedy sought in civil law cases. The second type of remedy asks the court to order certain behaviour from one party. For example, a court can grant an injunction to a cloud service provider requiring them to do or to desist from certain actions. The final type of remedy is a declarative remedy meaning that the court gives an opinion that does not require action by the parties but that sets out how the law applies to the facts, for example, or whether the contract gives rights to a third party or not.

Most civil actions for breach of contract seek damages as a remedy. However, some parties to a contract, particularly for a claim that involves divulgence of information, may seek an injunction to prevent publication of the information or to require the deletion of the information leaked. Actual remedies are determined on a case-by-case basis since the appropriate remedy depends on the facts of the case.

As regards cloud contracts, most consumers will probably not immediately seek legal redress by suing their cloud service provider under contract due to the cost implications, although this option is open to them. In the event that they do sue their cloud service provider, the option of having an award in damages may not be what would give them adequate redress for loss or accidental disclosure of personal data, for example.

Legislative sanctions

In the case of enforcement by public bodies, they also have the power to impose a penalty for breach of the law, which is not to compensate the victim of the breach, but to punish the wrongdoer. In the case of cloud computing, the most likely enforcement for breach by a public body will concern actions investigating breach of data protection law. While a customer may be glad that the wrongdoer is punished, a penalty on its cloud service provider does not provide it with any personal redress for any breach.

Redress and remediation outside the legal system

What most individuals that use Cloud computing services seek is often some way in which to have their complaint listened to and addressed by the cloud service provider itself. This may be that the complaint is fully investigated and all steps are taken to address whatever harm occurred to them. Redress and remediation methods that do not involve formal legal action may be more attractive for consumers or small businesses since it does not involve instructing lawyers. It may also achieve more for the customer, for example, a change in their cloud contract or it may give them more say in the type of redress they receive.

Even in terms of public enforcement, recent research suggests that audits by the data protection authorities on the best practices of cloud service providers yield good results as regards behaviour. For this reason, the privacy regulators may be moving from a reactive model of taking formal enforcement action after the breach, to a more proactive model which features regular, continuous audits.[110]

The aims behind this move are likely to be deeper than merely seeking new ways to supervise legal and regulatory compliance. The costs of any enforcement activity by a regulator, whether retrospective sanctioning for breach or proactive auditing to identify process defects which might lead to breaches, are inevitably very high. It is unfeasible to investigate, sanction or monitor more than a small minority of the players in cloud, so that improving the level of compliance requires what is effectively voluntary change on the part of all those who are under the regulatory radar, albeit backed up by the threat of possible sanctions or future audits.

Thus in our view, one of the consequences of this proactive model will be to change the mindset of cloud providers and data controllers. Auditing identifies good, and bad, practice, and both providers and controllers have an incentive to be recognised as adopting good practice, which is likely to attract customers, and avoiding bad practice, which will lose customers and create the risk of regulatory enforcement. The ability to demonstrate good practice is exactly what the accountability mindset aims at. By providing an account of data processing practices, providers and controllers disclose their failures as well as their successes. Unremediated failures will lead to civil claims, based on the disclosures which provide evidence of failure, and also potential regulatory sanctions using the same evidence. Thus an inevitable consequence of this transparency is that it has to be accompanied by mechanisms for providing redress to those affected. In effect, law and regulation cease to be business obstacles for those entities who adopt an accountability approach, and become instead guidelines as to the way the business should operate.

Of course, this change in mindset can only work if it is possible to provide the accountability information which customers, data subjects and regulators need. This is where A4Cloud's accountability tools come in. The adoption of incident management and governance approaches leading to more accountability by cloud service providers to customers in dealing with incidents or breaches of cloud security or data protection. One of the tools developed by the A4 Cloud project to identify incidents is the Incident Response Tool (IRT) that will alert the customer to a breach. In this way the cloud customer will be more empowered to seek redress and remediation for breach.

Conclusion on redress and remediation

The difficulties of redress and remediation in cloud environments arise from several factors. First, many cloud service providers will use their principal place of business as the basis for the legal system and the litigation forum governing their standard contracts with customers.[111]This means that many cloud services are offered under the laws of a particular U.S. state and include terms that try to restrict legal disputes to the courts of those states. Consumer law in the EU generally upholds the principle that clauses requiring a consumer resident in one country to be bound by the laws of another country are unfair and this is likely to apply to contracts with cloud consumers or with businesses acting as consumers.[112] The parties that are not protected by consumer law are small and medium-sized enterprises that enter into contracts with cloud providers. They rarely have the negotiation power to re-negotiate the choice of law or jurisdiction with their cloud provider, and yet they are not protected by EU consumer protection legislation.[113] Therefore they may be obliged by the cloud provider's standard contract to resolve disputes under foreign laws in foreign courts mainly in the U.S. The extra cost of obtaining legal advice for any dispute and the cost of litigating in a remote jurisdiction may discourage

them from seeking redress from their cloud provider. Second, many cloud providers seek to exclude as far as possible any warranty of service or acceptance of liability.[114]This means that data protection and privacy issues may have exclusions and disclaimers relating to them in the cloud provider's contract. In addition, few cloud providers are explicit as to the location or even geographical zone where the data is stored or the identity of any underlying service providers.[115]This means that many issues are unclear to Cloud customers on reading the standard cloud provider contracts. This lack of transparency and inability to get redress are factors that erode trust in Cloud services and require greater attention from Cloud providers and businesses preparing and providing such terms.[*]

[*] Redress and remediation are aspects of cloud accountability that are researched in the A4 cloud project and the software tools needed to demonstrate redress and remediation by cloud service providers are part of this work. For example, one way of helping cloud customers to obtain redress and remediation is to help them compare the cloud providers' contracts, the key terms and what these mean for their ability to have legal redress. This is addressed in the A4Cloud project by a tool called the Cloud Offering Advisory Tool (COAT). This enables the customer to compare various cloud offerings and to identify key issues such as data retention, applicable law, data protection and privacy issues are dealt with by the cloud service providers' contracts. By highlighting these terms, for example, applicable law and jurisdiction and explaining the significance of this in the cloud contract, customers are put in a better position when it comes to choosing a cloud provider that allows them means of seeking legal redress in local courts.

7 Integrating accountability tools with legal compliance

Although Cloud computing and similar Internet technologies have greatly grown in popularity over the past decade, consumer and business trust of the Cloud is greatly lacking, to say the least. A recent Netskope study, "Data Breach: The Cloud Multiplier Effect in European Countries" revealed that 72 percent of European businesses accuse cloud providers of failing to meet data protection and privacy standards, 77 percent of the businesses surveyed doubted that cloud providers would notify them straightaway if information was breached, and that 53 percent believed that use of the Cloud increases the likelihood of data breaches.[116]

Three of the most important reasons for this lack of trust are:

(a) Cloud customers and individuals whose data are stored and processed in the cloud have no information about what is actually happening with respect to their data. They are reliant on the promises made by cloud providers, but have no way of checking whether those promises are being fulfilled;

(b) Compliance on the part of a cloud provider relies heavily on human oversight of the internal processes which aim to achieve compliance. Those processes are usually collective in nature, ie all data is treated in the same way because of the difficulty in devising individualised policies which take account of the differing data protection and confidentiality needs for different items of data; and

(c) If there is a compliance failure, notification of those concerned and reassuring them that the failure has been remedied properly is also problematic because of the difficulty in determining *who* is affected and *how* they were affected.

All three of these issues are addressed by the accountability tools which A4Cloud is developing. These tools aim to provide information to users and data subjects (issue a), provide automated mechanisms which assist the cloud provider to comply with its legal and regulatory obligations at a granular level rather than purely collectively (issue b), and to automate the process of reporting breaches and their remediation to customers, data subjects and regulators (issue c).

It is, though, essential to recognise the limitations of these tools. As this deliverable has demonstrated, law and regulation is immensely complicated. It is not simply a system of rules which, if captured and coded properly, can be implemented into systems which ensure compliance. Rather, law and regulation begins from the perspective of norms and principles, which explain at a high level how a cloud provider *ought* to behave, and then expands on those with more detailed rules. Some of these detailed rules are potentially susceptible to automation[117], but others cannot because they embody non-computable open-textured concepts such as fairness and reasonableness.[118] Even those which appear to be computable may have a hidden open texture, because their application is always dependent on the individual context and thus their meaning can change from context to context.[119]
Surden summarises the position neatly:

> … legal practice is thought to require advanced cognitive abilities, but such higher-order cognition remains outside the capability of current AI technology. Attorneys, for example, routinely combine abstract reasoning and problem solving skills in environments of legal and factual uncertainty. Modern AI algorithms, by contrast, have been unable to replicate most human intellectual abilities, falling far short in advanced cognitive processes--such as analogical reasoning--that are basic to legal practice.[120]

This is not to say that automated tools cannot produce answers to the questions which the law poses. The emerging discipline of machine learning in law demonstrates that answers can be found. The difficulty is that a different process from that which the law uses produces these answers. To quote Surden again:

> For a certain subset of tasks, it may be possible to detect proxies or heuristics that closely track the underlying phenomenon without actually engaging in the full range of abstraction underlying that phenomenon … It is important to emphasize that such a

> proxy-based approach can have significant limitations. First, this strategy may only be appropriate for certain tasks for which approximations are suitable … Second, a proxy-based strategy can often have significant accuracy limitations. Because proxies are stand-ins for some other underlying phenomenon, they necessarily are under- and over-inclusive relative to the phenomenon they are representing, and inevitably produce false positives and negatives. By employing proxies to analyze or classify text with substantive meaning for an abstract task, for example, such algorithms may produce more false positives or negatives than a similarly situated person employing cognitive processes, domain knowledge, and expertise.[121]

Thus machine learning can be used to predict the answers which a judge or regulator might give in a particular situation, often with a high level of accuracy, but because the prediction is based on proxies it cannot explain the *justification* for that decision.[122] Justification is a fundamental element of the rule of law.[123]

Machine learning can also attempt to induce the implicit or unspoken rules on which a legal decision might be based.[124] The operative word here is *might* – the discovered rules are heuristics, or rules of thumb, and may be completely different from the implicit rules applied by a human decision maker, even if they produce the same results on a test set. Again, the necessary justification which characterises a legal decision is impossible.

What this tells us is that automated tools for accountability can *assist* greatly in achieving compliance, but because they cannot embody law accurately they cannot *guarantee* success. More work therefore needs to be done to understand the interactions lf law and accountability tools, and a detailed analysis of the role the A4Cloud tools will play in this enterprise will be undertaken in Deliverable D-4.12.

Failure to achieve perfect legal and regulatory compliance is unfortunate, but inevitable. To a large degree law is aspirational; it describes preferred behaviours and proscribes unwanted ones, but in practice recognises that humans and organisations will often fall short of the ideal. Thus when it comes to imposing sanctions for compliance failures, there is a great deal of enforcement discretion. Credit is given for good faith efforts to comply, even if those efforts were not completely successful, and compliance with the normative and principled aims of law and regulation may permit breach of specific rules to be treated leniently. Deliverable D-4.11 has analysed the aims and practices of data protection authorities when undertaking investigations, and indicates that rule compliance is only one of the issues with which they are concerned. Providing accountability is an important way for cloud providers to get closer to achieving the law's aspirations, and accountability tools make the achievement of those aspirations, or something close to them, far more likely to succeed.

8 Accountability through policy and legal governance

As we have seen, there are numerous legal considerations for Cloud providers, Cloud customers, and Cloud subjects to consider in their use of the Cloud. Although the strictest requirements arise from the law, in particular regulatory obligations and contractual obligations, sound legal governance also takes into consideration technological developments and tools, market and economic factors, and the cost and value of compliance. The legal drivers to incorporating these other considerations are primarily the open-texture[125] of many legal and regulatory obligations, which require cloud providers and users to act fairly and/or reasonably. Both fairness and reasonableness go beyond mere "tick-box" compliance with law and regulation; they require organisations to think about their activities in the context of their obligations, and where necessary change the way they operate to act in accordance with those obligations.

It is therefore important to recognise that accountability is far wider than mere legal compliance, and also that legal compliance requires making judgments about the proper way to act.[126] Clearly, a privacy policy or an account of a breach or system failure that fails to explain whether, and how, legal obligations are complied with is a defective account. This is where law and regulation fits into accountability. But it is also worth noting that because the precise requirements of law and regulation are so difficult to determine, certainly at a level which could be coded into cloud systems, adopting an accountability approach is likely to go a long way towards satisfying the law's requirement, or at least convincing regulators and enforcement authorities that legal and regulatory failures can be condoned or treated leniently.

Approaches to accountability

Practical accountability, for all intents and purposes, has been examined by other authors and projects, all of which have reached similar conclusions. Many of those authors were driven by the same general questions which can be summarised as:

> … does the organisation have an effective complaint handling process? Is there a responsible person, such as a Chief Privacy Officer? Is there a privacy management framework? Is there staff training?[127]

As noted, many scholars, privacy practitioners and others have tried to answer these questions. The Paris Project argued that there were five general elements in addressing accountability:

(1) Organisational commitment to accountability and adoption of internal policies consistent with external criteria
(2) Mechanisms to put privacy policies into effect, including tools, training and education
(3) Systems for internal, ongoing oversight and assurance reviews and external verification
(4) Transparency and mechanisms for individual participation
(5) Means for remediation and external enforcement[128]

The same project argued that there were nine fundamental activities that an accountable organisation should undertake:

(1) Policies
(2) Executive oversight
(3) Staffing and delegation
(4) Education and awareness
(5) Ongoing risk assessment and mitigation
(6) Program risk assessment oversight and validation
(7) Event management and complaint handling
(8) Internal enforcement
(9) Redress[129]

Determann;s comprehensive book, self-described as a “field guide” to starting a compliance program, selects compliance mechanisms, drafting documentation, and maintaining and auditing data privacy compliance programs as the main constituents of accountability.[130]

Furthermore, non-profit organisations are now dedicated to the promotion of data protection, privacy, and/or accountability. One such organisation, and a partner in the A4Cloud Project, is the Cloud Security Alliance, which has a mission statement “to promote the use of best practices for providing security assurance within Cloud Computing, and provide education on the uses of Cloud Computing to help secure all other forms of computing” and which, in part, certifies and registers cloud providers and the security controls offered by such providers.[131] Another such non-profit organisation is the International Association of Privacy Professionals, which certifies individuals as privacy professionals in different areas of privacy law, including European privacy, U.S. privacy, information technology, privacy management and other areas.[132]

Moreover, some standards have been developed and others continue to be developed with each passing day. Standards describe externally recognised norms adopted by a standards organisation or international or industry body.[133] There are various types of standards developed by both public standards organisations and private standard setting industry bodies. A technical standard specifies the full and often complex details of a format or protocol or interface and describes how to make things work in an interoperable manner. Alternatively, a standard can describe what is considered best practice in the industry as regards service quality, for example, including performance, security, privacy and availability. These types of standards, called evaluative standards, are often dependent on third-party certification to demonstrate compliance.[134] A certification scheme can be defined as the collection of requirements, procedures and means available for obtaining a certificate.[135] It has been defined as ‘the successful conclusion of a procedure to evaluate whether or not an activity actually meets a set of requirements’.[136] In relation to evaluative standards, which indicate that certain levels of quality or security have been met, a certification process offers an objective third-party assessment of compliance, which further generates trust among customers that the service attains the required standard.[137]

Organisations often write their policies based on evaluative standards. In respect of cloud standards, security standards have received a lot of attention recently since security concerns were identified as one of the main challenges when it comes to building trust and confidence in cloud services.[138] Challenges and risks particular to cloud security are identified in several studies[139] and in these studies references to cloud security include a wide range of issues including network and information security in general and are broader than purely protection of personal data.[140] Concerns about cloud security extend to infrastructure resilience, authentication, certification of processes and protection against illegal activities in the cloud environment including malicious system or data interference to the cloud users or service providers.[141] This wide range of issues is reflected in the draft standards that the International Standards Organisation (ISO) is debating on cloud security which addresses the issue for both customers and for cloud service providers.[142]

Finally, the Article 29 Working Party itself established a non-exhaustive list of similar types of policies and procedures, which included:

(1) Establishment of internal procedures prior to the creation of new personal data processing operations
(2) Setting up written and binding data protection policies to be considered and applied to new data processing operations
(3) Mapping of procedures to ensure proper identification of all data processing operations and maintenance of an inventory of data processing operations
(4) Appointment of a data protection officer and other individuals with responsibility for data protection
(5) Offering adequate data protection, training and education to staff members
(6) Setting up procedures to manage access, correction, and deletion requests which should be transparent to data subjects
(7) Establishment of an internal complaints handling mechanism
(8) Setting up internal procedures for the effective management and reporting of security breaches

(9) Performance of privacy impact assessments in specific circumstances
(10) Implementation and supervision of verification procedures to ensure that all measures not only exist on paper but that they are implemented and work in practice[143]

Swire and Kinesa have summarised the steps into three comprehensive stages:

> First, requirements result from identifying and assessing the security threats to and vulnerabilities of the organization. Second, legal, regulatory and contractual obligations can help an organization define security requirements. Third, the organization's principles, policies and objectives will further inform an organization's security requirements.[144]

Another notable and worthwhile approach for organisations to utilise, integrate into their own approach, and at the very least, consider, is the Privacy by Design concept originated by former Information and Privacy Commissioner Ann Cavoukian in the mid-90's.[145] That approach consisted of seven foundational principles:

(1) Being proactive, not reactive; and being preventative, not remedial
(2) Making privacy the default setting, i.e. not requiring any further action by users to maintain privacy
(3) Embedding privacy into design as a core element promoted throughout the organisation and to be considered at every stage of development
(4) Full functionality in considering all legitimate interests and objectives and trying to avoid trade-offs
(5) Beginning to end security through the entire life cycle of information
(6) Visibility and transparency to ensure that promises are being satisfied
(7) Prioritizing and respecting individual privacy

The definition of accountability developed by A4Cloud is the one we will use in the following analysis:

> Accountability consists of defining governance to comply in a responsible manner with internal and external criteria, ensuring implementation of appropriate actions, explaining and justifying those actions and remedying any failure to act properly.

In light of all of the foregoing, and taking into account the great amount of literature on this topic, and ultimately for the purposes of this paper, we split accountability and legal governance into five general segments: (1) learning and understanding the controlling legal requirements; (2) identifying risk; (3) establishing policy; (4) enforcing and adapting policy; and (5) remediation and redress.

8.1 Understanding the controlling legal requirements

Accountability begins with learning and understanding the controlling legal requirements and the corresponding legal duties and obligations, whether such obligations come from regulations or from contracts. This deliverable has attempted to explain the most salient of these at a level which is usable by cloud providers and users. However, the meaning of law and regulation is contextual, as we have previously explained, and so it is essential that cloud providers and users go beyond this general introduction and consider their particular circumstances. Legal advice will often be necessary to discover and understand more precisely the individual application of law and regulation.

In particular, further advice will always be necessary if:

(a) The cloud customer is doing things differently from the norm. Data protection and the law of confidence are built around very simple conceptual "business models", in which information is collected overtly from person A, used by the collector in some way (possibly involving sub-contractors who have no interest in the information), and perhaps disclosed to person B. Once

this model is departed from, individual advice will be needed to learn and understand the effect of the law. Typical examples might be covert collection or collection in ways person A does not understand, using information in a way which is not understood by person A, or involving sub-contractors who have their own interests in using the information.

(b) The cloud customer works in a sector which places a high value on privacy and confidentiality, such as health or financial services. These sectors tend to have specific sectoral regulation, which is likely to vary greatly from country to country.

Once the relevant legal obligations have been learned and understood, this leads directly into the next stage of identifying risk.

8.2 Identifying risk

Corresponding to the legal obligations and contractual duties is the identification and evaluation of risk factors. These are commonly referred to as privacy impact assessments (PIAs) and involve the use of checklists and /or tools to ensure that a company's information system is evaluated for risks of breach or other forms of unintended disclosure. Generally, the evaluation will examine all facets of the information life cycle from the collection of the information through the use of the information to the disclosure of the information to the storage of the information through the ultimate destruction of the information.

A common formula used for PIAs or other risk-assessments is:

Risk = Threat x Vulnerability x Expected Loss[146]

The National Institute of Standards and Technology has defined these terms in better applying the formula to the real world. Risk is defined as a measure of the extent to which an entity is threatened by a potential circumstances or event. Threat is defined as any circumstance or event with the potential to adversely impact organisational operations or assets. Vulnerability is defined as a weakness in an information system, system security procedures, internal controls or implementation that could be exploited by a threat source.[147]

This formula can be applied by cloud providers and others acting in the capacity of a data controller or data processor by utilizing not only security metrics, but applying a common-sense analysis of operations, the type of data being handled, and the risk of such data being breached or compromised. For security metrics, such analysis can include the number of breaches, number of outages, the number of times of unauthorised access, the amount of data being processed, the value of the data, the potential exposure and cost of addressing, resolving and/or remedying such breaches.[148] A common-sense approach can also look at how exposed such data is to potential unlawful access and the type of data, i.e. the risk of such data being accessed (for example, financial data would have a much greater risk of being accessed than other less innocuous data). Similarly, risks to data from internal threats needs also to be assessed.

It is also important to evaluate the flip-side of risk in relation to improperly using personal information or confidential information. These risks can generally be categorized into four categories: legal risks (facing litigation or regulatory action); reputational risks (facing deterioration of the brand and loss of customers based on breaches and/or lacking accountability and security measures); operation risks (the internal cost of breaches and/or misuse of personal information); and investment risks (ensuring that a company receives an appropriate return on processing personal information, especially when juxtaposed against evolving regulations and enforcement).

Unfortunately, computer hackers always seem to be one step ahead of the latest technology. This is perhaps best highlighted by the number of security breaches in just the last couple of years throughout the world. A recent study chronicled that there were 229 public data breaches since 2004 in the EU alone.[149] In the U.S., it almost seems like a weekly occurrence of a well-known company reporting some sort of data breach. One of the more notable of such breaches was the data breach discovered in late

2013 of major U.S. retailer Target from which criminals gained access to credit and debit card information, as well as customers' personal identifiable information with an estimated cost to Target of $148 million.[150] And, most recently, there was the wide disclosure of celebrities' photos, some of which were clearly intended to remain private. While many of those photos were purportedly stored in Apple's system iCloud, Apple released a media advisory stating that none of its systems were breached, and that instead, the accounts were compromised by "a targeted attack on user names, passwords, and security questions."[151] In other words, apparently even the largest of companies and all consumers with personal data and business with sensitive business information in the Cloud are at risk, regardless of the method of the attack.

Nevertheless, performing a risk assessment aids in identifying the types of risk, and further provides education and information about the details of the various types of risks, the levels of risk and the impact of risk. This risk assessment then needs to feed into a legal and regulatory risk assessment, because the open-textured obligations of fairness and reasonableness require steps to be taken to mitigate risks. Once the risks are known, the adequacy of the proposed steps can be assessed. It will rarely be possible to state with certainty that they achieve compliance, and thus the legal and regulatory assessment will identify residual legal risk to be kept under review. As an example, there is always a potential risk that anonymous data can be de-anonymised, at which point it would become personal data and give rise to obligations under data protection law. Developments in technology will constantly change that risk, thus changing the legal risk and the steps which are appropriate to handle such changes.[152]

Ultimately all this leads the provider and/or other business to the next step of establishing policy, standards and tools which are designed to manage both operational and legal risk.

8.3 Establishing policy, standards and tools

The establishment of policy is perhaps the most important step a Cloud provider will take towards increased accountability. A privacy policy can generally be defined as an internal statement that governs an organisation's handling of practices of personal and/or confidential data. The policy provides how the organisation will process such information, including collection, processing, storage, dissemination, retention and destruction, as well as the information security measures that are applied to such processing and breach management and notification.

In respect to information security, three overriding principles control: (1) confidentiality (how access to data is limited); (2) integrity (ensuring that data is authentic and complete; and (3) availability (the data is accessible, as needed, by those authorised to access it).

These three principles are practically addressed through three security controls developed through infrastructure, both physically and virtually: (1) physical (locks, security cameras, fences, etc.); (2) administrative (training, monitoring, incident response procedures, etc.); and (3) technical (automated controls and monitoring, firewalls, access control, logs).* Finally, from a high-level perspective, information security controls can be classified into three general types: (1) preventive (stopping incidents before they occur); (2) detective (monitoring for system anomalies); and (3) corrective (managing, mitigation and correcting a breach or incident after it has occurred). Importantly, while A4Cloud focuses on the technical aspects of these three controls, Cloud Providers must remain aware that such controls must also practically be employed through management, training and monitoring, and not just software or other technical measures.

Importantly, in implementing such policy the organisation should appoint a capable privacy or data protection officer. This is not only important in the pursuit of increased accountability, but many laws are now requiring the appointment of such an officer.[153] That officer should also be well-versed in the adoption of a privacy policy and the ongoing enforcement and adaptation of the policy to both internal and external developments. That officer should also be prepared to work with internal stakeholders in overseeing that the privacy policy is implemented and followed throughout an organisation, whether it be legal, information technology, management, security, customer service and/or public relations, as

* The focus of A4Cloud is largely based on the development and/or improvement of technical measures.

well as with external stakeholders and advisors, including legal counsel where there is not already experienced privacy counsel within the organisation.

As Determann[154] notes, one important consideration will be the level of documentation to be created within the organisation regarding the policy, enforcement and monitoring. Most companies use notices, consent forms (now often done electronically), agreements, protocols for internal processing, policies and other documentation related thereto, and documents required to be filed with data protection regulators. Critically, one focus of A4Cloud has been the creation of evidence through logs, audit trails, and other forms of tracking an organisation's accountability mechanisms. Such evidence and the electronic data and documents created through such mechanisms and tools is critical to accountability, as it allows for full transparency and allows the organisation to better understand why a breach has occurred, to prevent such breaches in the future, and ultimately, to account to the customer.

Ultimately, the aim of such policy is to manage the operational and legal risks previously identified. But of course, the policy may not achieve this aim. This is well-understood for operational risks, with the result that policies are normally reviewed several times to assess how well they deal with those risks. Change in legal risk is often overlooked, but requires the same kind of recursive review process if it is to be managed properly and incorporated into the accountability process.

An accountable organisation will encompass the general principles of the adopted policy into an external notice made available to its customers describing how the organisation collects, uses, retains, processes and discloses any personal information. The privacy notice serves two primary and important purposes: (1) it informs the customer about the more significant aspects of the privacy policy; and (2) it increases organisational accountability by setting a published standard which the company must satisfy, especially since a breach of that policy can expose a company to litigation and regulatory enforcement mechanisms (see section 6 above). Oftentimes, a company will publish the substantial majority of its privacy policy, though it is common for businesses to use a more simplified form and/or various levels of privacy notices such as a short form of notice (providing a general overview) and then allowing the customer to click through to more descriptive notices and/or layered notices addressing the more intricate levels of the company's privacy policy.

8.4 Enforcing and adapting policy

For Cloud providers, sound legal governance is generally viewed as effectuating safeguards to protect confidentiality, integrity and availability of data. Such protections arise from three areas: administrative steps, technical steps, and physical steps in effectuating proper safeguards within a company. Administrative steps include developing strong policies and safeguards and utilizing other administrative measures such as role-based controls to provide sound information security. Administrative steps also include policy enforcement, training, and enforcement of such policies. Technical steps include the use of technology, such as encryption, public key infrastructure, password management, authentication, tracking, non-repudiation, digital signatures and other technological tools to aid in data protection. Finally, physical steps are those steps that can be physically taken and which should not otherwise be forgotten by Cloud providers. Those steps include use of locks, perimeter controls and security monitoring. While companies are not required under any regulations to employ all measures available to them, they nevertheless should conduct a risk assessment in identifying the threat, vulnerability, and the expected loss in determining which measures should be taken and at what cost. Such an assessment and the resulting measures not only will serve to better protect the data entrusted to the Cloud provider, but it will also aid the Cloud provider in defending those measures in the event of a breach and, ultimately, to be a more accountable Cloud provider, the overriding goal of A4Cloud.

All of the foregoing takes hours of preparation, implementation, and ongoing monitoring and enforcement. Most Cloud providers should begin their compliance programs with the hiring and/or selection of a capable person as a privacy officer to oversee the entire program. This might not be a lawyer, but certainly a lawyer should be consulted to ensure that there is proper regulatory and contractual compliance and to ensure that contracts are properly negotiated and prepared. The lawyer will also be able to assist in an advisory role as to ongoing compliance, especially in tracking the evolving regulations and enforcement actions by various authorities. However, an effective policy, use of

available tools, and consistent monitoring and enforcement of the policy will help to ensure accountability, especially when faced with a system failure and/or data breach.

Cloud customers will want to ensure that the contracts entered into with Cloud providers provide adequate protection for service levels, audit rights, redress and remediation, and other contractual provisions to ensure that the Cloud provider is fulfilling its contractual and regulatory requirements. Again, use of a lawyer will be the best first step in such protections, especially in regard to preparing or reviewing, and negotiating any contract. Nevertheless, there remains many obstacles to the involvement of lawyers in this way, not merely financial but also cultural and in terms of non-financial resources like time. Tools which incorporate elements of legal governance, such as those being developed within the A4Cloud Project, can help to overcome some of these difficulties, even though they do not replace the complex evaluative and judgmental functions of lawyers.

Finally, Cloud users, i.e. individual consumers, will want to ensure that the Cloud provider and/or any business with which the user is dealing with which are conducting some business through the Cloud and collect, use or otherwise process personal information, have proper policies in place and that such companies ensure, at least through their privacy notices, terms and conditions, and/or contract that such personal information is processed for only the stated purposes and that proper remedies are in place should the Cloud provider or business utilizing the Cloud fail in their obligations. Accountability here includes providing individual consumers with information about how their data is processed and reassurance that the reality of processing matches. As we have seen, there are legal obligations to provide some information about these matters, and so the accountability mechanisms adopted need to pay special attention to ensuring that these legal obligations are met.[*]

8.5 Incident management and breach notification

We discussed redress and remediation in Section 6 above. As noted, redress and remediation, at least from a regulatory and contractual perspective, generally consists of rights, remedies, sanctions, fines, and forms of injunctive relief, i.e. compelling or restraining some type of behaviour. All such means of redress and remediation equally apply to the Cloud. However, we focus here on redress and remediation from the perspective of accountability and what A4Cloud has termed the 'notion of the account.' By this, we mean a Cloud provider and/or Cloud business accounting to the Cloud subject.

In the Conceptual Framework Deliverable[155], we examined this concept in the context of how does and/or should a Cloud Actor, generally a data Controller or Cloud provider, account to a customer regarding events, most often data breaches. The overview provided therein, in accordance with the conceptual framework of the A4Cloud Project, is more conceptual than practical. Here, we endeavour to examine the notion of the account from a more practical perspective, as it remains a critical aspect of governance and policy and oftentimes remains one of the only interactions between the cloud provider and the cloud customer and usually where the highest stakes exist in handling breach notification responsibilities.

Critically, there is no formal standard for data breach notification adopted by any of the official standard-setting bodies. Nevertheless, some guidance and methodology on data breach notifications has evolved in the EU since a European data breach notification requirement for the electronic communication sector was introduced by the ePrivacy Directive in 2002.[156]

Article 4 of the ePrivacy Directive imposed an obligation for the notification of personal data breaches by providers of publically available electronic communication services to competent authorities and affected individuals.[157] The European Commission, as required by the Directive, published implementing measures on the format, the procedure and the circumstances of the personal data breach notification.[158] The European Commission regulation set out a standard notification procedure and format to ensure that all electronic communication service providers subject to the Directive could take a pan-EU approach to data breach notification. This measure dealt more with the formal procedure

[*] This will be examined by A4Cloud later in the project in late 2015 in D44.6.

rather than assessing the severity of the data breach.

Guidelines on Data Breach Notification

In 2011, the European Union Agency for Network and Information Security (ENISA) reviewed the measures and procedures in EU Member States with regard to personal data breaches and it published a study on the technical implementation of Article 4 of the ePrivacy Directive.[159] This study included recommendations on: how to plan and prepare for data breaches, how to detect and assess them, how to notify individuals and competent authorities and how to respond to data breaches.[160] Its guidelines take into account best practices for preventing, managing and mitigating data breaches from the point of view of the data controller and industry providers. It also draws on examples of data breach notification from specific business sectors outside of electronic communication services (for example it looks at healthcare and financial services) to identify different approaches.

Methodology for Data Breach Notifications

In its guidelines on data breach notification in 2011 ENISA published a draft methodology for Data Breach Notifications in the Annex but with caveat that it needed further development. In 2013, ENISA, in collaboration with the Data Protection Authorities of Greece and Germany, published a methodology for data breach severity assessment that could be used by Data Protection Authorities and data controllers.[161] They plan to develop the methodology further with the aim of having a "final practical tool for a data breach severity assessment."[162] The proposed methodology is intended to provide data controllers with a quantitative tool to assess the severity of data breaches and notify the competent authorities.[163] The report also suggests that data controllers could use this methodology to determine how to mitigate data breaches. It could also provide national authorities with a tool or template to assess and report on the severity of breaches notified. The methodology involves assessing the severity of a breach by estimating the potential impact on individuals by examining three criteria:

- ***Data Processing Context (DPC)*** which addresses the type of data involved
- ***Ease of Identification (EI)*** which determines the ease of identifying specific individuals
- ***Circumstances of breach (CB)*** which relates to the type of breach and whether any malicious intent or purely accidental.

The level and severity of the breach is based on weighting given to these three elements.

The European Union Agency for Network and Information Security (ENISA) has usefully supplemented the EU legislation by producing guidelines on data breach notification, intended for communications providers subject to Article 4 of the ePrivacy Directive. As an off-shot of its guidelines it produced a methodology for assessing the severity of a data breach. The ENISA guidelines on data breach notification are specifically related to the electronic communication sector and compliance with Article 4, although they provide useful guidance and comparison with other sectors. The ENISA methodology for assessing data breach severity, on the other hand, is written to have general application for data breach assessment in all industries. Therefore, although there is no formal standard, there is a useful guidance that could be applied by data controllers in creating internal company policies on data breach notification.

In looking generally at the purposes of providing an account, there is little dispute that it is a central tenet of accountability as a legal obligation, as the account itself demonstrates accountability. As Gray and Jenkins opined:

> To be accountable is to be liable to present an account of, and answer for, the execution of responsibilities to those entrusting those responsibilities. Thus, accountability is intrinsically linked to *stewardship*. Stewardship involves two manifest parties: a steward or accountor, that is, the party to whom the stewardship or responsibility is given and who is obliged to present an account of its execution, and the principal or accountee, that is, the party entrusting the responsibility to the steward and to whom the account is presented. There is however, a third party in this relationship: the codes on the basis

> of which the relationship is struck and by which it is maintained and adjudicated. Codes may be explicit or more often implicit.[164]

As the oft-cited Charles Raab also noted:

> To 'give an account' – *rendre des comptes* – is to tell a story, and there are three levels that can be distinguished. First, on a weak definition, it means the obligation of an organization to report back, to 'give an account of its actions'. Second, on a stronger definition, it means that, plus the implication that the audience can interrogate the account and produce other accounts 'on their own account'. Third, on the strongest definition, it means the previous two plus the implication that sanctions can be brought to bear where there is a general agreement that the organization has 'given a bad account of itself', either (a) through its inactions, or (b) through its own unsatisfactory production of an account. The audience, which may be the public, can thus 'hold the organization to account', and that might have real consequences.[165]

And, as Raab further noted:

> But the account must also, and essentially, include descriptions and explanations of the actions, for two reasons. First, so that we can better understand the organisation's intentions and its understanding, or theory, of its own situation or how it might act in it. Second, because most of a steward's actions are invisible to the principal, and therefore have to be re-presented, through stories or accounts, explanations, and justifications.[166]

Importantly, especially for an organisation to be accountable, an account is not provided only when something has gone wrong, but rather can be presented at any time upon request. As one commentator opined:

> Accountability does not wait for a system failure; rather, it requires that organizations be prepared to demonstrate upon request by the proper authorities that it is securing and protecting data in accordance with the essential elements.[167]

Thus, for all intents and purposes, an account can perhaps best be defined, though simply, as 'a report or description of an event." It should sometimes include reasons, e.g. if the event should not have occurred, and explain consequences, e.g. what action will be taken for the future.

Despite the foregoing, there has been little specificity provided by regulators as to what accounts must contain, and likewise, most contracts in cloud computing also provide little details as to what an account must contain. As we saw above, little direction is provided in the Data Protection Directive, or even the proposed General Data Protection Regulation on this point.

As referenced above, the Article 29 Working Party ('Article 29 WP') has published its own opinion highlighting the importance of the notion in the field of personal data protection.[168] In its Opinion 3/2010 on the principle of accountability, the Article 29 Data Protection Working Party highlighted the importance of a concrete proposal for a general accountability principle. Specifically, the Article 29 Working Party found that accountability should focus on two main elements: "(i) the need for a controller to take appropriate and effective measures to implement data protection principles;" and "(ii) the need to demonstrate upon request that appropriate and effective measures have been taken. Thus the controller shall provide evidence of (i) above."[169] From a data protection point of view, the account is the method of presenting such evidence and demonstrating such measures.

The Article 29 Working Party also explained how the use of accounts will lead to greater enforcement by data protection authorities, and perhaps for our discussion, increased accountability:

> Furthermore, putting the accountability principle into effect will provide useful information to data protection authorities to monitor compliance levels. Indeed, because data controllers will have to be able to demonstrate to the authorities whether and how they have implemented the measures, very relevant compliance related information would be available to authorities. They will then be able to use this

> information in the context of their enforcement actions. Moreover, if such information is not provided upon request, data protection authorities will have an immediate cause of action against data controllers, independently of the alleged violation of other underlying data protection principles.[170]

A similar approach is taken in the non-binding 2009 Madrid international privacy standard, which also addresses the need for organisations to provide an account:

> The Responsible person shall: a) Take all the necessary measures to observe the principles and obligations set out in this Document and in the applicable national legislation, and b) Have the necessary internal mechanisms in place for demonstrating such observance both to data subjects and to the supervisory authorities in the exercise of their powers, as established in section 23 (Monitoring).

These documents are very important to the process of devising accountability mechanisms which deal with legal compliance. Although the documents are not law, they will inevitably influence courts and enforcement agencies in their assessment of whether legal compliance has been achieved. This is not to say that they are slavish templates, to be followed rigorously. Rather they are good practice guidance for accountability. It may be entirely appropriate to adopt a different accountability approach, and even a better way of dealing with the issue, but at the least there should be a consideration of these recommendations and a clear justification for adopting the new path.

Contracts in the Cloud and practical accountability

Contracts between data controllers and cloud users, and, to a lesser degree, contracts between data controllers and data processors also, do not shed much light on the notion of the account. Contractual obligations essentially take regulatory obligations, which may be at a high level, and translate them into specific binding obligations between the parties.[*] And even then, data controllers largely try to further limit their obligations, particularly their liability, in their contracts and/or terms of service.[171]

As between data controllers and data processors, Article 17 of the Data Protection Directive requires data controllers to impose on data processors the same obligations regarding the implementation of security measures as those imposed on data controllers. The relationship between data controllers and data processors will normally be established via the prior conclusion of a contractual agreement (or other legal act).[172] The initial draft of the Proposed Regulation stipulated in Article 26(2) that such a contract or legal act should be obligatory and should require the processor to "make available to the controller and the supervisory authority all information necessary to control compliance with the obligations laid down in this Article", or in other words to provide at least a partial account.

Finally, the one area where one would most expect an account to be provided would be where there has been a security breach, yet, even in negotiated contracts, as opposed to the standard, non-negotiated contracts which currently dominate the cloud computing landscape, "many providers' standard terms did not require reporting of security incidents and so on to users."[173]

It is noteworthy that even where accounts are imposed by law through legislation and contracts, there is most times little to no express provision as to what the account must specifically include. If accountability is to be built into the Cloud, an important element will be the inclusion of terms in contracts which require a proper account to be given.

It is not possible to draft model contract clauses for this purpose because what is proper in an account will vary substantially depending on the nature of the relationship between the giver and the recipient of the account. It is, however, possible to suggest some overriding principles which might guide the drafting of such clauses:

[*] It is also important to note that contractual obligations are not only based on regulatory obligations. Non-legislative obligations such as industry standards and certifications or even accepted industry norms can be included into agreements, which turn such obligations into legal contractual obligations.

(a) The recipient of the account should be entitled to appropriate information about how its data will be stored and processed, updated as storage and processing methods change. The level of detail will depend on the nature of the relationship and the data. Thus a consumer user of a "free" cloud service should be content with quite general information, whereas a financial institution will require far more detail.
(b) There should be a suitable mechanism for checking that the actual operations on data match the information given under (a). Mechanisms might range from tools which allow customers to generate their own reports, through independent audit reports, to a right to inspect and audit a provider's systems.
(c) There should be an appropriate mechanism for reporting breaches to those whose interests are engaged, primarily customers, data subjects and regulators. What level of reporting, at what seriousness of breach, and to whom, again will depend on the nature of the relationships.
(d) The account should include explanations of the reasons for any failings, and the measures which will be taken to prevent future failure. The frequency, granularity and addressees of this part of the account are also relationship-dependent,

The practicalities of the account

As the concept of accountability in the cloud takes hold, we foresee a time when failure to provide an account could expose a data controller or a data processor, depending on the specific circumstances, to a claim for breach of contract as well as to regulatory sanctions. But even now, as examined in greater detail below from a business perspective, it makes good business sense for data controllers to provide an account from time to time to their users, and likewise, data processors to data controllers. And where there is an alleged breach of applicable data protection regulations, the data controller is currently likely to be required to provide a report, i.e. an account, to the applicable data protection authority if the breach is detected. Voluntary reporting, in hopes of avoiding sanctions and/or minimizing such sanctions, is potentially a good strategy.

In light of the foregoing, an account, when required and/or provided, usually consists of the accountable actor providing a report or description of an event or process. The account should generally include the answers to what are traditionally referred to as the 'reporters' questions', i.e. who, what, where, when, why and how. Oftentimes, an account will also include the measures being taken to remedy a breach or failure. Still, the form and content of the account are contextually dependent and may be specifically dictated under the specific circumstances. Forms of the account may include Data Protection Impact Assessments, notifications to supervisory authorities, notifications to data subjects, contractual compliance verifications, audit reports, and even certifications and seals obtained by data controllers and/or data processors from third party certification agencies such as Cloud Security Alliance.

Applying these principles in practice perhaps best demonstrates the notion of the account and what would be encompassed in an actual account. Using Business Use Case 1 (BUC 1) from the A4 Cloud Use Case Descriptions Deliverable in WP B-3, it is easy to envisage multiple situations where an account might be necessary. BUC 1 concerns the flow of health care information from medical sensors to the cloud. The actors in BUC 1 include the business end users of healthcare organisations, individual end users of elderly persons using the sensors, cloud providers providing data storage and sharing, and the data regulator of the Norwegian Data Protection Authority.

One common situation where an account is required and provided is a data breach scenario. This scenario hypothesizes a breach of one of the cloud providers where data has been accessed and downloaded without authorisation. Critically, neither the Data Protection Directive, nor its implementation in Norway under the Act of 14 April 2000 No. 31 relating to the processing of personal data (Personal Data Act) requires a notice of the security breach to be provided to any of the other actors, namely the Norwegian Data Protection Authority or the data subjects. Such notification may be required under Norwegian regulations. Regardless, as an accountable Cloud provider, the provider here desires to provide an account to the user and the Norwegian Data Protection Authority.

To the end users, the account would likely be sent by email, but depending on the severity of the breach, notice could and quite possibly should also be sent by mail to ensure proper notice and receipt. As noted above, the account here should encompass answers to the fullest extent possible of the reporters'

questions, i.e. who, what, when, where, how and why, as well as measures being taken to prevent such breaches in the future. More specifically, the cloud provider will want to (1) explain who committed the breach, if known, or that further investigation is being undertaken to ascertain who committed the breach; (2) what the breach consisted of and the extent of the information that might have been accessed, i.e. health information, financial information, etc.; (3) when the breach occurred and was discovered; (4) where the breach occurred; (5) how and why the breach occurred, if known, what security measures in place, whether those security measures were properly working at the time of the breach, and how the breach generally circumvented such measures; (6) what measures were taken to ascertain the extent of the breach; (7) what measures are being taken to prevent such breaches in the future; (8) contact information for a department or person to respond to any further enquiries regarding the breach; and (9) perhaps a link to a web page where further information, if any, will be disseminated regarding the breach and any further investigation.

Thus, hypothetically and a its basic form, an account by a Cloud customer and/or Cloud provider to Cloud subjects after a data breach may appear as follows:

Dear End User:

We write to regarding a recent unfortunate incident involving an unauthorized access to our servers in which your personal data may have been accessed.

On February 1, 2014, we believe that an outside intruder circumvented our security measures and was able to access the personal information of some of our users. We realized the access almost immediately and were able to minimize the access. The full extent of the breach is not known, or whether your information was accessed and/or otherwise obtained by the intruder. What we do know at this time is that our security measures were operating properly, but the intruder was able to circumvent such measures through illegal means. We have since closed the means through which the access occurred and are re-examining all of our security measures to ensure the fullest protection available moving forward. We are also continuing to investigate the situation and further exploring the extent of the information which may have been accessed.

We will release further pertinent information regarding our investigation on our website at www.cloudprovider.com/01022014breach, so we invite you to regularly check that page for any updates regarding this situation. Should you desire to contact us for further information, please do so at [email] or [telephone number], where we will be standing by to respond to any enquiries as quickly as possible.

We thank you for your continued patronage and your confidence in us preventing these unfortunate incidents in the future.

Sincerely,

Cloud Provider

Thus, to the end user, the account will be more general and simpler language, without much of the technical information that would otherwise be available to the cloud provider. The cloud provider may decide to include more technical information on its website or upon request by the end user, but the overriding objective to the end user should receive a clear explanation of the account.*

* The same may not be said for the account of the same breach to the Norwegian Data Protection Authority. There, the account likely should contain more technical information, the extent of the breach, a more technical overview of the breach, and the number of persons impacted by the breach. The account should also include relevant evidence regarding the breach, i.e. any applicable logs, audit trails, system maintenance records, and any other technical evidence regarding the proper operation of the cloud provider's security measures and the extent of the breach.

As more information is obtained by the Cloud provider and/or business, such information should continue to be provided through updated accounts to the end user. Returning to the handling of the data breach by U.S. company Target referenced above in section 8.3 provides a prime example of such accountability in practice. Target established a webpage containing rather detailed information after its credit card processing systems were compromised.[174] It continued to update that page providing its customers with information about the extent of the breach, measures which were being taken to prevent such breaches in the future, and other precautions end users should take to avoid damages and/or further damages. The account and updated accounts by Target provide an excellent template for companies facing similar data breaches and/or circumstances in the future.

8.6 Concluding thoughts as to accountability and governance

In sum, there are multiple factors to consider in implementing sound governance in order to increase accountability in the Cloud. As seen above, businesses utilising the Cloud to conduct business must first examine and try to understand the legal requirements that apply to them, which as we have seen, is generally based upon the jurisdictions in which they are conducting business and targeting end users, especially individuals. As we have also seen, once those legal requirements are understood, the applicable risk can be evaluated, which can simply be summarised as analysing the threat, vulnerability and expected loss, but which can be a complicated exercise based on the numerous factors that go into each category. Once that process is completed, policy and corresponding standards can be formulated, including the physical, administrative and technical safeguards which can be implemented to minimize risk of security breaches and/or the negligent disclosure of personal or confidential information. As we have also seen, businesses cannot simply stop there, as they must consistently ensure that the policy is enforced and that the policy be adapted as circumstances change and risk increases. Finally, where there is an incident, the management of such events becomes critically, including the notification and ongoing account to the Cloud subject.

9 Conclusions

The reader who has managed to get to this point might reasonably have gained the impression that law and regulation is complex, difficult to understand and implement, and constantly changing its meaning. All this is unfortunately true. Law attempts to regulate human behaviour, and needs therefore to be as complicated and unforeseeable in its effects as that behaviour is.

Nonetheless, there is hope. Although sections 2-6 demonstrate the difficulties which law presents to Cloud actors, these difficulties arise mainly at the level of detail. The fundamental principles of the law are clear and simple, and not overly complex. Our first conclusion is thus that accountability needs to focus most strongly on demonstrating that the fundamental principles of law have been complied with. An account of this type might be all that individual data subjects need, but this would not be true for some categories of Cloud customer or for regulators. As an extension of this conclusion, we suggest that accountability needs to be layered based on the complexity of the Cloud activity and the relationships involved. In simple terms, as a Cloud business's activities increase in scope and range, so should the layers of accountability it provides and the information contained in those accounts.

Our second conclusion is that accountability methods and tools can play an important part in achieving such accountability. The law is concerned with what should have been done, what was actually done, and who was responsible for any failures. In a complex technical infrastructure which is distributed geographically and involves multiple actors, such as the Cloud, generating and sharing this information can only be achieved through technological solutions. Without accountability tools the Cloud is a black box to the law; its internal workings need to be visible for law to achieve its social purposes. And it is therefore important that those methods and tools be designed so as to assist the legal and regulatory compliance process and provide the information that process needs.

Our next conclusion is that accountability tools are one part of a larger mosaic, which has to include mechanisms for development of policy and governance processes which ensure that policies are appropriate to achieve compliance and are actually put into effect. Law and regulation is one input into policy and governance. Accountability tools are another crucial input, as well as providing many of the mechanisms which implement policy.

If law, tools, policy and governance are designed to work together, a high degree of accountability is achievable. And, as we explained in section 6, accountability changes the mindset of Cloud actors towards legal compliance, making it more likely and reducing the need for remediation and redress. Thus our final conclusion is that law should be designed with accountability in mind, precisely so as to secure these advantages.

10 References

[1] See eg *Google Spain v AEPD* (Case C131-12 2014), 13 May 2014.
[2] Proposal for a Directive of the European Parliament and of the Council on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure, COM(2013) 813 final, 28 November 2013.
[3] Google Spain v AEPD, Case C131-12, 13 May 2014.
[4] Ibid at footnote (fn) 1.
[5] See generally Chris Reed, *Making Laws for Cyberspace* (Oxford University Press: Oxford 2012).
[6] Regulation (EC) 44/201 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (Brussels), OJ L12/1, 16 January 2001; Regulation (EC) 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I), OJ L177/6, 4 July 2008; Regulation (EC) 864/2007 of the European Parliament and of the Council of 11 July 2007 on the law applicable to non-contractual obligations (Rome II), OJ L199/40, 31 July 2007.
[7] *Zippo Manufacturing Co. v. Zippo Dot Com, Inc.*, 952 F.Supp. 1119 (W.D. Pa. 1997).
[8] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data Official Journal L 281, 23/11/1995, pp. 31 – 50. (Hereafter referred to as the 'Directive' and/or the 'DPD').
[9] As of mid-2013, 99 countries had some sort of data protection framework, but over half of those nations adopted such laws after the year 2000, showing the recent increase in such legislation. See Global Tables of Data Privacy Laws and Bills (3rd Ed, June 2013), UNSW Law Research Paper No. 2013-39.
[10] The package of reform proposals published by the European Commission on 25 January 2012 is available at http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm
[11] Viviane Reding, 'Strong and independent data protection authorities: the bedrock of the EU's data protection reform' (Spring Conference of European Data Protection Authorities, Luxembourg, 3 May 2012) SPEECH/12/316 <http://europa.eu/rapid/press-release_SPEECH-12-316_en.htm>.
[12] DPD, Art. 2(a).
[13] DPD, Art. 8.
[14] Article 2(d) DPD.
[15] Article 2 (e) DPD.
[16] DPD, Art.17.
[17] WP169, Opinion 1/2010 on the Concepts of 'Controller' and 'Processor', WP 169 (2010).
[18] W. Kuan Hon, Christopher Millard and Ian Walden, 'Who is responsible for 'personal data' in cloud computing?--The cloud of unknowing', Part 2 (2012) 2 International Data Privacy Law, 3.
[19] Article 4(1) (a) DPD.
[20] Article 4 (1) (b) DPD.
[21] Article 4 (1) (c) DPD.
[22] See Article 29 Data Protection Working Party, 'Opinion 8/2010 on applicable law', 0836-02/10/EN, WP 179 16 December 2010.
[23] Article 25(6) DPD.
[24] Published by the European Commission at http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm.
[25] Hon and Millard 'How do Restrictions on International Data Transfers Work in Clouds?' Chapter 10 in Millard, *Cloud Computing Law* (OUP 2013, Oxford).
[26] Article 26 (4) DPD.
[27] Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council (2010/87/EU0, [12 February 2010] OJ L39/5.
[28] Hon and Millard, p.267.
[29] Ibid, p 268.
[30] For a detailed examination of BCRs see Lokke Moerel, *Binding Corporate Rules: Corporate Self-Regulation of Global Data Transfers* (Oxford University Press 2012).
[31] Article 28 DPD.
[32] Vranaki (editor), 'The Rise of Investigations by European Data Protection Authorities in the Context of Cloud Computing' Deliverable for D4.11 in A4Cloud project, 30 September 2014, at 15-23.
[33] Millard et al, Cloud Computing Law (2013, OUP Oxford) Part III Protection of Personal Data in Clouds (pp165-282).

[34] Hon, Millard, Walden 'What is Regulated as Personal Data in Clouds ?' Chapter 7 pp 167-192 in Millard et al.
[35] *Opinion 4/2007 on the Concept of Personal Data, WP 136* (2007).
[36] Ibid.
[37] Hon, Millard, Walden 'Who is Responsible for Personal Data in Clouds ?' Chapter 8 pp 193-219 in Millard et al.
[38] A29WP, *Opinion 1/2010 on the Concepts of 'Controller' and 'Processor'*, WP169 (2010).
[39] A29WP, *Opinion 05/2012 on Cloud Computing*, WP196(2012)
[40] Hon, Millard, Walden ibid, 208.
[41] A29WP, WP 196 (2012).
[42] Hon, Millard, Walden, ibid. 203.
[43] For a thorough discussion of this subject, see Hon, Hörnle and Millard 'Which Law(s) Apply to Personal Data in Clouds ?' Chapter 9 in Millard et al.
[44] Hon and Millard 'How do Restrictions on International Data Transfers Work in Clouds ?' Chapter 10 p 254-282 in Millard et al.
[45] DPD Art 25(1).
[46] Hon and Millard, ibid, p.255
[47] The public sector is often timid in their approach to cloud services as shown in the EU-funded study conducted by IDATE and Technopolis for the European Commission, 'Analysis of cloud best practices and pilots for the public sector' and 'Annex to the final report: Country files', A study prepared for the European Commission DG Communications Networks, Content & Technology, 2013, see http://ec.europa.eu/digital-agenda/en/news/analysis-cloud-best-practices-and-pilots-public-sector.
[48] http://ec.europa.eu/internal_market/iprenforcement/docs/trade-secrets/120113_study_en.pdf
[49] http://europa.eu/rapid/press-release_MEMO-13-1061_en.htm
[50] *Fraser v Thames TV* [1984] QB 44.
[51] *Attorney General v Guardian Newspapers Ltd* [1990] 1 AC 109; see also, *R v. Department of Health ex parte Source Informatics* [2001] QB 424 (CA).
[52] *Fraser v Thames TV* [1984] QB 44.
[53] *Cantor Fitzgerald International v Tradition (UK)* (2000) RPC 95; *Mars UK Ltd. v Teknowledge Ltd.* (2000) FSR 138.
[54] *Ryan v Capital Leasing* (High Court of Ireland, 2 Apr. 1993).
[55] *Prince Albert v Strange* (1849) 2 De G & Sm 652.
[56] See eg *Franchi v Franchi* [1967] RPC 149 (information lost its confidential status where the information was published in a foreign patent application).
[57] *Initial Services v Putterill [1967] 3 All ER 145, [1968] 1 QB 396.*
[58] *Attorney-General v Guardian Newspapers (No.2) [1990] AC 109; see also, English & American v. Herbert Smith (1988) FSR 232* (holding a third party coming by confidential information innocently, but subsequently discovering the information to be confidential, will be bound by a duty of confidence).
[59] *Shelly Films v Rex Features* (1994) EMLR 134.
[60] [1960] RPC 128.
[61]Proposal for a Directive of the European Parliament and of the Council on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure 2013/0402 (COD), http://ec.europa.eu/smart-regulation/impact/ia_carried_out/docs/ia_2013/com_2013_0813_en.pdf.
[62] p. 6 Proposed Directive on Trade Secrets.
[63] Alan Cunningham and Chris Reed 'Consumer Protection in Cloud Environments' in the book Millard et al, Cloud Computing Law (2013, OUP).
[64] Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market.
[65] Articles 6 and 7.
[66] Direction 2000/31/EC of the European Parliament and of the Council of the 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce').
[67] Article 1(2) of the Directive on electronic commerce defines information society services as any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services.
[68] Article 5 of Directive on electronic commerce.
[69] Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights.

[70] Direction 2000/31/EC of the European Parliament and of the Council of the 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce').
[71] Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights.
[72] Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market.
[73] Annex I to the Directive, the "Black List". Also see guidance document from the European Commission consolidating practice on this Brussels, 3 December 2009 SEC(2009) 1666 Commission staff working document Guidance on the implementation or application of Directive 2005/29/EC on Unfair Commercial Practices and available at http://ec.europa.eu/justice/consumer-marketing/files/ucp_guidance_en.pdf.
[74] Cunningham and Reed, ibid, at 338.
[75] Ibid.
[76] Articles 9-13 of the Consumer Rights Directive
[77] Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts.
[78] Article 6(1).
[79] Australian Privacy Commissioner press release 14 August 2013, http://www.oaic.gov.au/news-and-events/media-releases/privacy-media-releases/privacy-commissioner-website-privacy-policies-are-too-long-and-complex. The average reading age of the policies surveyed was 16, whereas the Commissioner's recommendation is that the policy's reading age should be 14, and the average length of policies was 2,600 words, again considered excessive.
[80] Decision and Order, *In the Matter of GeoCities, Inc.*, FTC File No. 98203915 (Feb. 12, 1999), www.ftc.gov/os/1999/02/9823015.do.htm.
[81] Decision and Order, *In the Matter of Eli Lilly & Co.*, FT File No. 012-3214 (May 10, 2002), www.ftc.gov/os/1999/02/9823015.do.htm.
[82] Decision and Order, *In the Matter of Gateway Learning Corp.*, FTC File No. 042-3047 (Sept. 17, 2004), www.ftc.gov/os/caselist/0423047/040917do0423047.pdf.
[83] Decision and Order, *In the Matter of Google Inc.*, FTC File No. 102-3136, (Mar. 30, 2011), www.ftc.gov/os/caselist/1023136/110330googlebuzzagreeorder.pdf.
[84] Decision and Order, *In the Matter of Facebook, Inc.*, FTC File No. 092-3184 (Nov. 29, 2011), http://ftc.gov/os/caselist/0923184/111129facebookagree.pdf.
[85] *Federal Trade Commission v. Wyndham Worldwide Corporation, et al.*, Case No. 2 :13-cv-1887 (ES-JAD), U.S. District Court, District of New Jersey, Doc. No. 181 filed April 7, 2014.
[86] www.whitehouse.gov/sites/default/files/privacy-final.pdf.
[87] http://ftc.gov/os/2012/03/12032privacyreport.pdf.
[88] See generally, Bradshaw, Simon, Millard, Christopher, and Walden, Ian (2013), Standard Contracts for Services, Cloud Computing Law, ed. Millard, C. 37 – 72.
[89] See Study on Trade Secrets and Confidential Business Information in the Internal Market, Final Study, April 2013, Prepared for the European Commission, Contract Number: MARKT/2011/128/D at p. 10.
[90] California Business and Professions Code sections 22575 – 22579.
[91] California Business and Professions Code section 22946 et. seq.
[92] Massachusetts 201 CMR 17.00.
[93] Revised Code of Washington Chapter 19.255.
[94] Millard et al, 37.
[95] Bradshaw, Millard, Walden 'Standard Contracts for Cloud Services', Chapter 3, pp 39-72 in Millard et al.
[96] Ibid, 71.
[97] Hon, Millard and Walden 'Negotiated Contracts for Cloud Services', Chapter 4 pp 73-107 in Millard et al.
[98] Ibid, 75.
[99] Ibid.
[100] Ibid 80-104 gives a detailed analysis of the cloud contract terms.
[101] Ibid 80-82.
[102] Ibid 82-83.
[103] Ibid 83.
[104] Gleeson and Walden 'It's a jungle out there.? 'Cloud computing standards and the law' ssrn.com/abstract=2441182
[105] Ibid 85.

[106] Ibid 90-91
[107] Ibid 91-96
[108] Ibid 97-99
[109] Ibid 78-79.
[110] Asma Vranaki, Paper for D4.14
[111] Bradshaw, Millard and Walden 'Standard Contracts for Cloud Services' in Millard, *Cloud Computing Law* (OUP, Oxford 2013), at 68.
[112] Cunningham and Reed 'Consumer Protection in Cloud Environments' in Millard, *Cloud Computing Law* (OUP, Oxford 2013), at 352-354.
[113] They might be protected in those EU countries which also have legal controls over inappropriate contract clauses in contracts between businesses, which might include choice of law and jurisdiction clauses, but the precise application of those laws to such clauses is uncertain until it is tested in court action.
[114] Bradshaw, Millard and Walden, ibid, at 68.
[115] Ibid, at 69.
[116] http://www.scmagazineuk.com/most-european-businesses-don't-trust-cloud-services/printar----
[117] See eg HP Privacy Advisor, where 300 pages of privacy policy were encoded and are involved in assessment within a decision support system – Siani Pearson, Simple Mode: Addressing Knowledge Engineering Complexity in a Privacy Expert System, HP-2010-75.

[118] See Mireille Hidebrandt, "Prefatory Remarks on Human Law and Computer Law", (2013) Ius Gentium 1, 6:

> … the inherent ambiguity of natural language may be lost in computing languages. This may require a conscious effort to achieve a measure of 'calculated' ambiguity. Neural networks, on the other hand, may generate new types of ambiguity, based on the unpredictability of their output and the incomprehensibility of what goes on between input and output.

See also Harry Surden, "Computable Contracts" (2012) 46 U.C. Davis L. Rev. 629, 646.
[119] See Richard Susskind, *Expert Systems in Law* (Oxford University Press: Oxford 1987); Neil MacCormick, 'Legal deduction, legal predicates and expert systems' (1992) 5 International Journal for the Semiotics of Law 181.
[120] Harry Surden, "Machine Learning and Law" (2014) Washington Law Review 87.
[121] Surden, n120, 97.
[122] Ibid 102 ff.
[123] See Lon Fuller, *The Morality of Law* (Revised ed, New Haven: Yale University Press 1969) Ch 2.
[124] See eg Martin Mozina, Jure Zabkar, Trevor Bench-Capon and Ivan Bratko, "Argument Based Machine Learning Applied to Law" (2006) 13 Artificial Intelligence and Law 53.
[125] See Frederick Schauer, *Playing by the Rules* (Oxford: Clarendon Press 1991), 36:

> Open texture is the ineliminable possibility of vagueness, the ineradicable contingency that even the most seemingly precise term might, when it confronts an instance unanticipated when the term was defined, become vague with respect to that instance. No matter how carefully we may try to be maximally precise in our definitions … some unanticipated event may always confound us.

[126] A4Cloud examined accountability in greater detail, and with less of a legal focus, in D32.1, Report detailing conceptual framework, including without limitation, in sections 4 through 7 therein.
[127] Bennet, C., 'International privacy standards: Can accountability ever be adequate?'. *Privacy Laws & Business International Newsletter*, August 2010, Issue 106, pp. 21-3, at p. 22.
[128] Hunton & Williams LLP, The Centre for Information Policy Leadership, 'Demonstrating and Measuring Accountability – A Discussion Document, Accountability Phase II – The Paris Project, October 2010', p. 3.
[129] Ibid at p. 10.
[130] Determann, Lothar, Determann's Field Guide to International Data Privacy Law Compliance, Edward Elgar Publishing Limited, 2012.
[131] https://cloudsecurityalliance.org/ (last visited October 8, 2014).
[132] https://privacyassociation.org/ (last visited October 8, 2014). This website provides a great resource to ongoing developments and issues in the areas of data protection and privacy law and compliance all over the world.
[133] Ian Walden and Niamh Gleeson "It's a jungle out there. Cloud computing standards and the law" May 23, 2014). Available at SSRN: http://ssrn.com/abstract=2441182

[134] Ian Walden and Niamh Gleeson "It's a jungle out there. Cloud computing standards and the law" May 23, 2014). Available at SSRN: http://ssrn.com/abstract=2441182
[135] ENISA, *Security certification in practice in the EU* (October 2013), 6 ('ENISA 2013').
[136] Casper, C., & Esterle, A., *Information Security Certification: A Primer: People, Products, Processes*, (ENISA, December 2007) 2
[137] Ibid, Walden and Gleeson.
[138] IDC (2012) 'Quantitative Estimates of the Demand for Cloud Computing in Europe and the Likely Barriers to Take-up' referenced in the Commission Communication and the accompanying Staff Working Document.
[139] Such studies include ENISA 'Benefits, risk and recommendations for cloud security' November 2009, at: http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment; Cloud Security Alliance 'The Notorious Nine: Cloud Computing Top Threats in 2013' February 2013, at: https://downloads.cloudsecurityalliance.org/initiatives/top_threats/The_Notorious_Nine_Cloud_Computing_Top_Threats_in_2013.pdf; Cloud Standards Customer Council ' Security for Cloud Computing' August 2012, at https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf.
[140] Cloud Security Alliance 'The Notorious Nine: Cloud Computing Top Threats in 2013' February 2013, at: https://downloads.cloudsecurityalliance.org/initiatives/top_threats/The_Notorious_Nine_Cloud_Computing_Top_Threats_in_2013.pdf; Cloud Standards Customer Council ' Security for Cloud Computing' August 2012, at https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf.
[141] Ibid.
[142] Draft standard on cloud security available at http://www.iso27001security.com/html/27017.html. This is unlikely to be finalised before 2015.
[143] Article 29 Data Protection Working Party, Opinion 3/2010 on the principle of accountability, 13 July 2010. WP 173, paragraph 41.
[144] Swire, Peter P. and Ahmad, Kenesa, Foundations of Information Privacy and Data Protection, A Survey of Global Concepts, Laws and Practices (2012) International Association of Privacy Professionals at 79.
[145] Privacy by Design: The 7 Foundational Principles," Office of the Information and Privacy Commissioner of Ontario, rev. January 2011, www.privacybydesign.ca/content/uploads/2009/08/7foundationalprinciples.pdf.
[146] Swire, P. and Ahmad, K, Foundations of Information Privacy and Data Protection – A survey of Global Concepts, Laws and Practices at p. 80.
[147] National Institute of Standards and Technology at http://nist.gov/ (last visited November 11, 2014).
[148] Ibid.
[149] Howard, Phillip N., Data Breaches in Europe: Reported Breaches of Compromised Personal Records in Europe, 2005 – 2014, Center for Media, Data and Society, October, 2014 at http://cmds.ceu.hu/sites/cmcs.ceu.hu/files/attachment/article/663/databreachesineurope.pdf (last visited on October 12, 2014).
[150] See http://www.forbes.com/sites/samanthasharf/2014/08/05/target-shares-tumble-as-retailer-reveals-cost-of-data-breach/ (last visited October 12, 2014).
[151] http://www.apple.com/pr/library/2014/09/02Apple-Media-Advisory.html (last visited on October 12, 2014).
[152] See also D36.2 Prototype for the data protection impact assessment tool undertaken in A4Cloud by the C6 Work Package, including the related work referenced in section 1.1 therein.
[153] For example, Germany has required a data protection officer since the early 1990s. BDSG, Federal Data Protection Act 1991, Council of Europe Doc. CJ-PD §36 (91) 30 (July 12, 1991).
[154] Determann, L. at fn. 130.
[155] D32.1 – Conceptual Framework (2014).
[156] Article 4 of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) OJ [2002] L 201, 31/07/2002 pp 37-47.
[157] Ibid. Note that this measure may be extended beyond the electronic communications sector if the current proposal to reform EU data protection law is adopted. A proposal for a general obligation of the data controllers for the notification of personal data breaches under certain conditions has been introduced in Article 31 in the draft EU Regulation on the Protection of Personal Data.
[158] Commission Regulation (EU) (EU) No 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, OJ [2013] L173, 26.6.2013

[159] ENISA report, *Data breach notifications in the EU*, published 13 January 2011 and available at https://www.enisa.europa.eu/activities/identity-and-trust/risks-and-data-breaches/library/deliverables/dbn and accessed on 13 October 2014.

[160] Ibid.

[161] ENISA, *Recommendations for a methodology of the assessment of severity of personal data breaches*, 13 December 2013 available at https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/dbn-severity and accessed on 13 October 2014.

[162] Ibid, Executive Summary.

[163] Ibid, Introduction, p 1 Objectives.

[164] Gray, A. and Jenkins, W., Administrative Politics in British Government, Brighton: Wheatsheaf Books, 1985, p. 138 (emphasis in original).

[165] Raab, C. (2012). The Meaning of 'Accountability' in the Information Privacy Context. In Managing Privacy through Accountability, ed. D. Guagnin et al., MacMillan, pp. 15-32 (citing Bovens, M., 'Analysing and assessing accountability: a conceptual framework', European Law Journal, 13, 4, pp. 447 – 68, at p. 448, 2007.).

[166] Id.

[167] Hunton & Williams LLP, The Centre for Information Policy Leadership, 'Data Protection Accountability: The Essential Elements – a Document for Discussion', October 2009, p. 10.

[168] Article 29 Working Party, "Opinion 3/2010 on the principle of accountability", WP 173, 13 July 2010.

[169] Id. at p. 28.

[170] Id. at p. 60.

[171] See generally, Bradshaw, Simon, Millard, Christopher, and Walden, Ian (2013), Standard Contracts for Services, Cloud Computing Law, ed. Millard, C. 37 – 72.

[172] Data Protection Directive Article 17.3 *The carrying out of processing by way of a processor must be governed by a contract or legal act binding the processor to the controller and stipulating in particular that: the processor shall act only on instructions from the controller,*

[173] Hon, W. Kuan, Milard, Christopher, and Walden, Ian (2013), Negotiated Contracts for Cloud Services, Cloud Computing Law, ed. Millard, C. 73 – 107.

[174] See https://corporate.target.com/about/shopping-experience/payment-card-issue-FAQ (last visited November 8, 2014).

CLOUD ACCOUNTABILITY PROJECT

Selected Bibliography

Article 29 Data Protection Working Party, Opinion 3/2010 on the principle of accountability, 13 July 2010. WP 173, paragraph 41.

Charlesworth, A. & Pearson, S. (2012). "Developing Accountability-based Solutions for Data Privacy in the Cloud". 26 (1), Innovation, Special Issue: Privacy and Technology, *European Journal for Social Science Research*, pp. 7-35. Taylor & Francis, UK.

European Parliament (2012). "Fighting Cyber Crime and Protecting Privacy in the Cloud". Directorate-General for Internal Policies. http://www.europarl.euopa.eu/RegData/etudes/join/2012/475104/IPOL-IMCO_ET(2012)475104_EN.pdf

European Parliament (2013). "The US surveillance programmes and their impact on EU citizens' fundamental rights". Directorate-General for Internal Policies, PE 474.405.

Kuner, Christopher, Transborder Data Flows and Data Privacy Law (Oxford University Press 2013),

Millard C (ed), *Cloud Computing Law* (Oxford University Press 2013).

Moerel L, *Binding Corporate Rules: Corporate Self-Regulation of Global Data Transfers* (Oxford University Press 2012).

Nymity Research (2014). "Implementing and Demonstrating Accountability." http://www.pcpd.org.hk/privacyconference2014/files/9_booklet_guide.pdf

National Conference of State Legislatures website at http://ncsl.org (contains overviews and regular updates as to U.S. state laws regarding data disposal, security breach notifications, and identity theft statutes).

Office of the Information and Privacy Commissioner of Alberta, Office of the Privacy Commissioner of Canada, Office of the Information and Privacy Commissioner for British Colombia (2012). "Getting Accountability Right with a Privacy Management Program." http://www.oipc.bc.ca/guidance-documents/1435

Pearson, S. & Wainwright, N. (2012). "An Interdisciplinary Approach to Accountability for Future Internet Service Provision." *International Journal of Trust Management in Computing and Communications (IJTMCC)*, 1(1) pp. 52-72.

Reed, C, *Making Laws for Cyberspace* (Oxford University Press: Oxford 2012).

Van Alsenoy, B. (2012). "Allocating responsibility among controllers, processors, and "everything in between": the definition of actors and roles in Directive 95/46/EC." *Computer Law & Security Review*, 28, pp. 25-43.