Public Consultation by the EU Commission on Cloud Computing

*Our Response*
Contents

Introduction
   Where is cloud computing? 3

Responses to the Commission's questions
   Profile 5
   Clouds for users 10
   Legislative Framework 12
   Embracing Interoperability 19
   Public sector clouds 19
   Future research and innovation programmes 19
   Global solutions for global problems 19

Appendix 1
   About Allen & Overy 21

Appendix 2
   Your Allen & Overy Contacts 22
Introduction

Our TMT practice, which is comprised of lawyers across our international network, has specialist expertise on agreements relating to the provision of services using Information Technology. Our work is typically multi-jurisdictional in nature.

We act across the world for numerous major financial institutions and corporate clients, as well as service providers, giving us a particular understanding of the challenges faced in relation to cloud computing, both from the perspective of the users and the providers.

We welcome this opportunity to respond to the Commission's consultation on cloud computing. In drafting our response we have been mindful of the views of our clients across several jurisdictions in which we advise.

Where is cloud computing?

We see cloud computing as the next generation of infrastructure and software application technology and view it as an integral element of today's technology used by consumers and enterprise customers alike. It is evolving at a fast rate.

The cloud has the potential to offer great benefits to both consumers and to businesses of all sizes. In today's world, where a focus on new technology sits alongside an ever-present requirement to cut costs, the cloud offers an attractive operating model. Cloud computing can offer anytime, anywhere access, speed, flexibility and "elasticity" – fully scalable solutions that can be used "on demand". The user only pays for what he orders and uses. This results in reduced pressure on internal systems and the potential to save or free-up valuable IT resources. It also offers potentially better security systems and back-up than can be procured in a self-sourced model.

As many commentators have pointed out, use of cloud services does have its challenges. The relatively uninhibited flow of data, often around the globe, has led to concerns over security, the location, transfer and handling of personal data and the protection of trade secrets. Other concerns include the possible difficulty of transition between providers and issues related to intellectual property rights management and choice of law. A decision to use cloud offerings will require careful planning and analysis in order to realise and maximize the benefits.

But it is our firm belief that the issues can all be solved, often quite easily. As often happens when new technology emerges, people tend to think about problems ("can we conclude an agreement by telex", "by fax", "by email" etc. – looking back, many concerns that were voiced when these 3 new technologies appeared in peoples lives were actually non-issues). We should seek to avoid the cloud being brought down by hype, confusion and over cautiousness.

While the cloud may not be suitable in every scenario, it is clear that it will continue to gain momentum and it is likely that industry consolidation and convergence, and the increased focus on this area by bodies such as the European Commission, will result in the adoption of standards and/or limited amendments to existing laws and regulations. Many of our clients feel that EU and government policies should be designed to encourage the growth of cloud computing and avoid imposing unnecessary barriers to its deployment and use. If care is taken, the benefits can be realised without harming consumers or undermining privacy, security or data protection regimes.
We believe that cloud computing should be embraced as a powerful and beneficial technology. As one of our clients has pointed out, cloud computing is "not a new or unique technology but rather represents the natural evolution of storage, consumption and delivery of IT computing services". It flows naturally from the increased availability of broadband communications throughout the world. The challenges are not therefore new. As such, we do not believe that it requires an entirely new or different set of laws or rules but rather current legal regimes which affect the use of cloud services should be amended where required.

Allen & Overy LLP

30 August 2011
Responses to the Commission's questions

1. Profile

Please see Appendices 1 and 2 for information about Allen & Overy.

Our clients include users, potential users and providers of cloud services.

Allen & Overy itself is also using some cloud services, and is investigating further use.

1.1 If you are a user of cloud services: Please describe your current use of cloud computing. What kind of problems do you encounter when using cloud computing solutions in the EU? Elsewhere?

In our experience, the following are the main problems encountered by our clients who are users of cloud computing – these are not necessarily unique to cloud computing but existing risks are sometimes heightened by the nature of the service offerings:

Ability to exit/move to another provider

Vendor lock-in and the natural dependencies arising from the provider/customer relationship can lead to challenges when a customer attempts to exit the relationship and transition to another provider. This is certainly not unique to cloud computing and in some other models (like certain types of outsourcing) it may be more difficult to exit than in the cloud. However, cloud computing technology and the cloud computing providers’ business models can make it difficult for the customer to leave. Additionally while existing cloud providers are prepared to negotiate their customer terms which relate to moving to another service, the value proposition offered by cloud computing often means there is less room for negotiation than in traditional information technology service arrangements. Larger, global institutions may have more bargaining power than smaller enterprises when trying to obtain protections around a smooth exit and data extraction.

Jurisdictional risks

Cloud computing may pose jurisdictional risks. While many global customers will be used to dealing with risks associated with a particular jurisdiction or working across jurisdictions, smaller customers may not be used to having to deal with the potential for legislative or regulatory intervention in the context of a globally distributed service.

Customers have raised concerns that they do not fully understand the implications of jurisdictional risk in cloud computing. Their number one concern is often that their data could exist anywhere within a globally distributed cloud computing platform at any particular point in time, and that depending on the technology, they may have no ability to pinpoint the location of their data. Providers have started to address this concern and some providers are now ring-fencing where their servers will be located for particular offerings to attract these potential users and help alleviate their concerns and hybrid cloud technologies (enabling the integration of a public and private cloud) are also being suggested as a solution for customers who have sensitive data requirements.

Performance related risks

As with any external service provision, customers contracting with providers are exposed to risks relating to the provider’s ability to perform the services to the required level. Many existing providers offer “best endeavours” service levels but are not prepared to accept an absolute contractual obligation to meet the service levels (or financial service credits associated with failure). In an internally hosted environment, depending on the scale of service required, a customer may implement measures to control performance issues. In more traditional service provision arrangements (or if the customer of cloud
services is a large corporate with great leverage he) can generally negotiate hard service levels and service credits to encourage good performance.

Though not particular to cloud computing, enterprise adoption of cloud solutions can expose individuals and organisations to increased risk of service disruption because of the variety of software vendors involved in cloud solutions and the remotely distributed nature of the solutions. A good example of this is where a provider is subject to an injunction for IP infringement and there are no readily available alternative technologies. Another example is where providers are unable to provide services to their customers due to a breach of licence terms with their key technology vendors. Similarly, there is an increasing reliance on telecommunications networks to access the services (and given the wider distribution of cloud services there are more “links in the chain” that can fail). To protect against this exposure, cloud customers should not view cloud services as an all or nothing proposition and may wish to consider engaging or retaining some degree of skill and resource (staff and computing resources), or even certain business critical functions, internally to protect against service disruption.

Control risks
Cloud users are exposed to requirements to comply with a number of laws and want the ability to understand and comply with applicable legislation (as mentioned in the paragraph on Jurisdictional risks above). Users also want to ensure that the data stored by a cloud provider will be secure. However they may have limited or no control over the security measures taken, the processing of the information and sometimes little idea where the information is hosted.

To address these concerns, providers are coming up with different offerings, such as ones which only hold data in certain jurisdictions or which offer increased security. While security breaches do happen, they are rare among cloud services and are generally quickly controlled.

Customers can also improve their position by putting in place protection which is adequate to address the sensitivity of the data, for instance through encryption of the data before storing it in the cloud (and where feasible, using a private cloud). Additionally it may be advisable to obtain regular back-ups of data. A customer should also be selective with regard to which services are outsourced to a provider. To mitigate the control risks (and risks of the unknown) potential users would also be well advised to conduct thorough due diligence on the provider, how and where they hold data, their security policies, and how they will enable the user to comply with applicable laws (such as data protection legislation). Contractual protections will back this up (where they can be obtained) and a customer with sufficient bargaining power can seek suitable obligations and liability provisions such as around loss of data.

If carefully designed, the security of the cloud is likely to be of a higher standard than any one company can achieve on its own.

Use of Intellectual Property
Users are often concerned whether the provider is granting them all the IP licences that they need to use the services effectively, especially for the software in software as a service (SaaS) agreements. Where the provider implements software solutions from third party vendors, the user may also wish to seek an indemnity for IP infringement. This is particularly important since standard software licence agreements are not always clear with respect to the licensees’ rights to offer the relevant software as a service. Also, issues on the use of open source software and the relevant licence terms should be considered. Providers are likely to want the indemnities to be limited and containable and may wish to seek an indemnity from the user against claims resulting from contents stored on their cloud (including for the infringement of third party intellectual property rights). Providers will sometimes argue that their offering is an infrastructure and that the customer should not worry about the provider having its shop in order, however they do realise that this may need some time.
Lack of leverage in the marketplace

Tensions exist in the cloud computing market which may make it more difficult for customers to engage with providers on a reasonable commercial basis. Cloud providers often sell their services in a commoditised way like a utility. This may mean they are reluctant to negotiate detailed contractual provisions. Of particular concern to our clients who use (or have considered using) cloud services is the customer's inability to negotiate controls within the contract in order for them to address compliance with legal and regulatory obligations.

As we can see from the issues listed above, the challenges faced by users of cloud computing are not generally new. They are common to many types of commercial agreements in the information technology sector. Many of them can be addressed through practical measures and choosing the right cloud offering. In many cases they are not an issue with the laws and rules which exist within the EU and elsewhere. Where challenges faced by users could be alleviated by alterations to existing legislation, this is often already being considered, for example in the revisions currently being considered in relation to the Data Protection Directive.

1.2 If you are a potential user but not active yet: What are the main reasons for not (or not yet) using Cloud Computing?

While adopting a cloud service may appear desirable in circumstances where scalability, flexibility and cost-benefit can be achieved, some of our clients find that a cloud based approach is not always the most suitable model. This is particularly where significant organisational and technical change is required (which also has an associated up-front cost), or where the risks of moving core business services into the control of a third party service provider outweigh the apparent benefits.

As further described above, some of the often cited disincentives to cloud adoption include:

- concerns over the ability of the cloud platform to protect personal information and financial data adequately;
- concerns over lack of clarity around the location of customer data;
- concerns relating to the lack of contractual commitment from providers in standard cloud contracts, particularly in relation to data loss and service levels;
- vendor lock-in concerns and concerns relating to the "stickiness" of the service and inability to move to a different provider. There is the potential that, without proper due diligence, this will become worse as a customers moves further up the cloud services stack, i.e. from infrastructure as a service (IaaS) to SaaS, and it may prove difficult to leverage further cost savings as the cloud services market matures;
- cost concerns relating to the integration of the services into existing service platforms. The challenges in moving existing integrated applications and services into the cloud are that they may require development work to re-factor the application for hosting in the cloud. This may be costly to achieve, and may not achieve any improved service levels or cost reduction benefits. The likely opportunity and entry point for using IaaS and platform as a service (PaaS) cloud services is likely to be in the establishment of "new" services and applications, rather than lifting and shifting the old systems onto a cloud platform.
- technology issues, particularly at the enterprise user end of the spectrum as particular enterprise applications may not be able to be run on cloud platforms due to the underlying technology used;
- pricing issues, particularly for large enterprise customers who can achieve similar unit pricing without using cloud offerings because of existing scale. In order for unit prices to fall there must be significant convergence and consolidation in the market so that there is sufficient scale to reduce overall price;
Some software vendors are being **slow in adopting an effective licensing model** for the cloud, a multi-tenanted (shared services) environment. This may lead to infringement of licenses when the product is used in the cloud and to pricing issues;

- **Fear of change**/the unknown and an associated perceived lack of control.

### 1.3 If you are a provider of cloud services: Please describe your offer. What kind of barriers do you face in providing your cloud computing services within the EU? Elsewhere?

Although Allen & Overy is not a provider of cloud services, in our experience of advising our clients (and seeking their views for this Response) providers face a number of challenges with their offers. These tend to mirror the concerns of the customers and as such are not generally new challenges or particular to cloud computing.

To put the barriers we list below in context, a good example of the types of initiative on which these barriers may impact is that of the cross-industry consortium which includes major Hollywood studios, retailers and consumer electronics manufacturers called the Digital Entertainment Content Ecosystem. This consortium has developed UltraViolet, an initiative that will permit consumers to access their own cloud-based digital rights “locker” enabling them to stream or download authorised copies of films and television shows they have previously acquired from UltraViolet retailers. Consumers will be able to obtain UltraViolet authorised content from multiple retailers, store the content either in the cloud or in devices that they own and play that content interchangeably on multiple device brands. The UltraViolet initiative, which should provide benefits to content suppliers, device manufacturers and consumers, represents the kind of business models made possible by cloud computing. Providers of these types of services feel that European and government policies should encourage such initiatives, and not make them more difficult to launch and operate by imposing (or failing to eliminate) the barriers listed below.

**Barriers encountered by some of our clients include:**

**Overly restrictive data security obligations**

Providers face a challenge in trying to ensure data security and related data protection requirements are met in a regulatory landscape which they feel is often unnecessarily restrictive. However, many of our clients also note that cloud computing may in fact offer better security solutions than when data is processed and stored at the individual data controller’s facility or in a single location by an off-site vendor. Customers that are subject to special security requirements, such as the obligations outlined in recent decisions of the Federal Trade Commission in the US or data protection regimes in the EU, will demand that their providers comply with those requirements. One client commented that "contractual requirements and best practices are likely to provide better and more flexible protection than specific legislated mandates that apply only to cloud computing services, which are likely to increase cost and lead to a patchwork of security measures instead of consistent protection of data wherever it resides”.

**Uncertainty about IP issues**

The lack of harmonisation of certain IP laws, and uncertainty in the application of IP laws to new technologies or new ways of doing business, creates difficulties with global offerings such as cloud computing. For example, in some EU countries there is a personal copying right under copyright laws, but this is not presently the case in the UK (although the UK government has recently announced plans to address this point). This means that certain cloud computing offerings may, if hosted in the UK, cause users to infringe if they copy their files (e.g. music files) onto a cloud while in France they would be covered by a personal copying (format shifting) exemption.
Governing law and Jurisdictional Issues – risks associated with uncertainty as to what laws apply and which courts resolve disputes
Like commercial parties in other fields, our clients (whether users or providers) generally try to agree in advance which law will apply to their obligations and which courts will resolve any disputes. They then set out these choices clearly in their contracts.

Of course, matters may not always be this straightforward. For example, if parties do not agree these matters in advance how does one ascertain in a cloud contract:

- the governing law of any contractual or non contractual claims, and
- which courts might take jurisdiction for such claims?

Ascertaining which rules to apply to determine which governing law applies (or, as the case may be, whether a court has jurisdiction) depends, firstly, on which forum is considering the question. Within member states a common approach to such issues is more likely given the existence of certain European instruments: Rome I and Rome II which set out uniform rules regarding, respectively, the governing law of contractual obligations and non contractual obligations and the Brussels Regulation which sets out uniform jurisdictional rules for the courts of Member States to apply.

Once one has ascertained the correct rules to apply, further complexities may arise when seeking to apply these rules. For example, in a negligence claim against a provider for loss of data in a cloud under Rome II the general rule is that the governing law of any non contractual obligation is the law of the place of damage. Where is the place of damage in the cloud? Is this where the data is stored? If it is, how is this place ascertained by the user if the data has been sent by a provider to a subcontractor? Is it where the financial loss of the user is sustained? (there are other rules potentially applicable – e.g. Article 5 product liability and Article 8 regarding certain intellectual property rights).

Claims may also fall outside these instruments meaning, even within Europe, there will be differences in approach to governing law and jurisdictional issues. For example, the approach of an English court in respect of a claim brought by an English user about cloud space bought from a US provider (in circumstances where there is no jurisdiction clause) may vary from the approach of a French court in respect of a French user who did the same thing. Of course, our clients will also often need to consider how these issues are considered by non member state courts.

Even where the parties have chosen the governing law and the courts to resolve disputes in their contract, uncertainty can arise because these choices may be overridden, subject to statutory exceptions, or be otherwise unenforceable. Certain clients have indicated a desire for more certainty that their contractual choices as to governing law and jurisdiction will be upheld i.e. there should be greater emphasis on upholding party autonomy and less scope for choice of law or court clauses to be overridden (see further below).

Conflicts of law
The requirements imposed by laws in EU member states can conflict with laws, and the demands of regulators and other law enforcement authorities, in foreign jurisdictions. It is not always possible to reconcile the obligations applicable to a provider in one jurisdiction with the obligations of the provider and/or customer in other jurisdictions, including the EU.

For example, US authorities can (and frequently do) demand access to data that is accessible by providers in the United States, pursuant to the USA PATRIOT Act 2001 and similar legislation; if that data includes personal data, it is possible that any such disclosure could cause a provider to breach data protection laws and regulations in one or more member states of the EU. Under the USA PATRIOT Act 2001 a provider based in the US or with a US subsidiary can be required to disclose: (i) any data to which the US entity has access, including any such data which is controlled and/or was collected by affiliates outside the US; and (ii) any data which is controlled and/or collected by any non-US subsidiary of the US
company (i.e. if the US company is the parent of any other company). The data required to be disclosed could include business records and, in certain circumstances, telephone and email communications.

Data can also be required to be disclosed, under compulsion of law, in connection with legal proceedings, as part of a pre-trial discovery process.

For entities operating in highly regulated sectors, such as financial services, this can prove a particularly difficult issue due to the degree of oversight exercised by regulators. Foreign regulators and law enforcement authorities have an increasing appetite for access to data (including personal data) held by banks and other financial institutions in particular.

It should be noted that under the French Blocking Statute the production, communication (whether in writing or orally) of financial, commercial, industrial, economical or technical documents and information from France for a legal action abroad is not permitted unless such production or communication is made in compliance with the applicable international treaties/conventions (e.g. with respect to hearings to be held in the United States, the Hague Convention relating to the Taking of Evidence Abroad in Civil or Commercial Matters must be complied with). Failing to comply with the French Blocking Statute triggers criminal sanctions (18,000 Euro fine and/or 6 months imprisonment).

Uncertainty about telecoms regulatory requirements.
See paragraph on Telecoms regulatory law below.

2. Clouds for users

2.1 Do you feel that in the cloud services you are currently using or have been evaluating (or are providing), the rights and responsibilities of both user and provider are clear?

The rights and responsibilities of both user and provider are relatively clear. However, there is some room for improvement. The obligations on the provider are still too often "best endeavours" only, with limited service levels. But cloud computing is still relatively new technology and service providers are generally reluctant to negotiate their standard terms and conditions, even when dealing with large enterprise customers. This is largely due to a relative lack of contention and a degree of immaturity in the market. This will change as competition increases and enterprise customers enter the cloud market and in the future there will be opportunities for those customers with scale to negotiate terms further.

We are seeing that cloud providers are starting to appreciate this tension and in a more competitive market have more recently released suites of offerings with terms which do deal with concerns such as security and data protection. Customers will want to check carefully whether the contract meets their legal requirements, mitigates any risks and otherwise addresses their operational and governance concerns.

2.2 Are you aware of the applicable jurisdiction in different types of disputes that could arise during your provision or use (or potential future use) of specific cloud offerings?

Many providers offer cloud services which span international borders. As mentioned above, where service provision is geographically diverse, there is potential that more than one legal or regulatory regime will apply. This situation is not unique to cloud computing. Generally most commercial parties will seek to agree a governing law (for contractual and non contractual obligations) and an exclusive jurisdiction provision in a cloud computing services contract to ensure that there is as much certainty as possible as to where disputes are resolved. There is often some negotiation on this point but, at least with commercial parties, there is generally perceived to be a benefit in classifying in advance where a dispute should be resolved. A provider may wish to set the forum for similar reasons. Problems may arise in some situations:
Consumer contracts

In contracts with consumers there are restrictions on the ability of parties to agree a governing law (Rome I, Rome II) and a choice of court to resolve disputes (the Brussels Regulation).

As to contractual governing law, under Article 6 of Rome I the choice of a particular governing law in a contract with a consumer will (broadly) not deprive a consumer of any protections afforded to him by provisions that cannot be derogated from by agreement under the law of the place of the consumer's habitual residence. This rule is however subject to its own exceptions. This means, in short, a chosen law may be overridden.

As to non contractual governing law, Article 14 of Rome II appears to restrict agreements (made prior to any damage) as to the governing law of any non contractual obligations arising out of or in relation to a contract to parties "pursuing a commercial activity" (Rome II also sets out rules regarding governing law of non contractual obligations regarding product liability and infringement of intellectual property rights).

As to jurisdiction, under Article 16 of the Brussels Regulation, a consumer may bring proceedings against a provider either in his home court or where the provider is domiciled. A provider may however only bring proceedings against the consumer in the consumer's home court.

Thus, when a provider wishes to offer its services to consumers in many countries, it must assume the risk of the potential application of numerous other (non chosen) laws. It also assumes the risk of having to seek redress against the consumer only before the consumer's home court and the potential uncertainties of it being sued before that court.

Breach of Jurisdiction clauses/Jurisdiction races

Parties do not always stick to the terms of their agreed choice of court agreement and instead seek to secure some tactical advantage by initiating proceedings in a non chosen court (perhaps one that is perceived to be more favourable and often one that moves slowly). There has been much debate elsewhere on the abuse of the lis pendens rules in the Brussels Regulation and the use of the so called "torpedo actions" (see for example Allen & Overy's response to the Commission's Green Paper on the recasting of the Brussels Regulation). We do not repeat the debate here save to say that we welcome the Commission's proposals to reform these rules which will no doubt assist parties operating in cloud computing and elsewhere achieve greater legal certainty in their contractual arrangements.

IP infringement

IP disputes may arise in the context of cloud computing e.g. if the user stores infringing works in the cloud. Since the parties cannot choose the applicable law for a non-contractual obligation arising from an infringement of an intellectual property right (article 8 para. 3 of the Rome II Regulation, principle of territoriality), an owner of an IP right must either sue the alleged infringer in its country of domicile or assert its claims separately for every state where that IP right is alleged to be infringed. In the case of registered IP rights, where the validity of the right is challenged, then the IP right owner will most likely have to assert its claims separately for every state where that IP right is alleged to be infringed.

Data protection

Article 4 of the Data Protection Directive (Directive 95/46/EC) provides that national laws not only apply when the controller is established within an EU member state, but also where it is using equipment located within the EU in order to process data (unless for "mere transit" purposes). The Article 29 Working Party recently provided guidance determining applicable law under Article 4 (opinion 8/2010), which clarifies what is meant by an "establishment" of the controller, and what is meant by "use of equipment", a concept which is interpreted broadly in many member states and may produce a result where data protection laws apply even though the processing has no real connection with the EU (or a specific member state). The Opinion suggests that further clarification is required as part of the revision of the general data...
protection framework but that trying to apply one law to all establishments of a data controller (that of the main establishment) would require a great degree of harmonisation across member states. We agree with this view, but nevertheless such an approach would offer much greater certainty and greatly reduce the administrative barriers to, and costs associated with, cloud solutions.

2.3 Is there an alternative approach to the determination of jurisdiction that may work better both for users and providers?

In relation to data protection specifically, when the customers of online services are based in the EU, data subjects retain the protections of the local laws of the jurisdiction in which the relevant data controller is established (the so-called "country of origin" principle) regardless of where data is stored or processed.

However, at a global level, we would welcome progress on the sign up to/ratification of the Hague Convention on Choice of Court Agreements. Widespread sign up/ratification of this Convention would provide greater certainty for our clients regarding the efficacy of their jurisdiction clauses and thereby boost confidence for those engaged in cross border trade.

As noted above, there is uncertainty about where damage might be said to have occurred in a cloud contract where there has been a loss of data – an important issue when seeking to ascertain the governing law of any non contractual obligations under Rome II. Guidance in this regard might be helpful.

In the consumer context, the Commission may wish to consider, perhaps as part of its work on the reform of the Brussels Regulation, the extent to which it might be appropriate for more weight to be placed on express agreements as to governing law and choice of court. For example, what if a party enters a contract as a consumer but then uses the cloud for commercial purposes? Should the provider be required to sue that party only in its home court under Art 16? When dealing with consumers in multiple jurisdictions some clients have expressed concern about the lack of certainty about the extent to which a governing law clause might be overridden in such consumer contracts. Concerns also arise about lack of certainty with respect to any choice of governing law of non contractual obligations (see above).

2.4 Do you feel that the question of liability in cross-border situations is clear for cloud users and cloud providers?

This depends on the provisions in the agreement. If carefully drafted, it should ensure clarity.

3. Legislative Framework

3.1 Do you think there are updates to the current EU Data Protection Directive that could further facilitate Cloud Computing while preserving the level of protection? If yes, please describe

Data protection challenges in relation to cloud computing stem predominantly from the fact that the legal framework for data protection was created in the context of a far less distributed vision of computing than exists today. Cloud computing is a further evolution of such distributed computing.

An update to the legal framework which adapts the legal requirements to the practical issues of modern use of technology, including cloud computing services, is important for users and providers of cloud services in the EU to remain competitive. However, we do not believe that this should lead to specific regulation of cloud computing. Those of our clients who gave us their views on this issue did not view cloud computing as a unique sector – such as financial or health information – that warrants its own set of rules or requirements, whether more generally or specifically in relation to data protection. There are inherent risks with specific regulation of a service model such as cloud computing in that such regulation, if not drafted with flexibility in mind, will soon become outdated and ineffective or worse unintentionally restrictive.
Roles of controller and processor:
The EU Data Protection Directive recognises a subdivision between data controllers and data processors. Customers will almost always act as a controller, whereas providers can act as controller or processor, depending on the nature of services provided. In some cases, cloud providers will act as controllers, if they exercise autonomy in relation to the manner in which and the purposes for which data are processed. Conversely, providers are likely to be characterised as data processors where they are processing data solely for the purposes of providing services to the customer (and solely in accordance with its instructions). Providers may prefer this characterisation on the basis that, in the capacity of data processor, they will generally have fewer (if any) direct obligations under European data protection laws (although the obligations of processors vary between member states). However, acting as a processor can also tie the hands of a provider (for example, see "EU transfers outside the EEA" below).

In relation to arrangements where providers act as joint data controller, together with the customer, clarification of the respective roles and responsibilities of joint controllers may help to avoid disputes as to liability and responsibility for processing.

In relation to arrangements where providers act as data processors, greater harmonisation of the laws applicable to processors across member states would be helpful in ensuring consistent treatment of cloud providers' activities across different member states. However, harmonisation should not merely result in the adoption of the highest standard across the member states.

EU transfers outside the EEA
Our clients view the issues with data transfers as not unique to cloud computing. The current regime is bureaucratic, as well as ineffective in ensuring any genuine enhancement of the protection of personal data when transferred cross-border. Restrictions on the movement of data between jurisdictions, and associated administrative requirements, for cloud computing and other legitimate business purposes, should be relaxed. Failure to do so will hamper the potential of cloud computing and other engines for global economic growth in the European Union.

In the context of cloud computing, customers and providers are generally not able to fall within the limited derogations to the general prohibition on cross-border transfers outside the EEA. Transfers are rarely "necessary" for performance of a contract – the transfers merely enhance the flexibility of the offering from the provider's perspective. Consent is an impracticable solution – this has been confirmed by the Article 29 Working Party's recent Opinion on the meaning of consent. The rights of data subjects to withdraw consent, and the need to obtain a positive indication of consent, means that it is typically not a workable option; in any event, it is not a preferred derogation by national data protection authorities as it does not ensure the protection of data outside the EU. Equally self-assessment of adequacy, where permitted by the laws of a member state, offers insufficient certainty and remains prohibitively costly, time-consuming and administratively burdensome. Furthermore, it is particularly difficult to self-assess adequacy in the cloud environment, where disparate service provision is involved, involving multiple providers across potentially wide areas and subject to different applicable laws and operating different systems and controls in relation to the protection of data.

As such, most customers must rely on the use of model contracts to legitimise transfers of personal data outside the EEA and the other adequate jurisdictions in connection with obtaining cloud services. The model contracts framework is not, however, fit for purpose, particularly in relation to the cloud. Acting as a processor under model clauses can tie the hands of a provider. For example, under the 2010 controller-processor model clauses, a provider acting as data importer must comply with onerous provisions in order to appoint sub-processors, which include an obligation to enter into sub-contracts on the same terms as the model clauses, to assume liability to third party data subjects and to provide a copy of its sub-processing agreements to the data exporter. It is not possible for cloud providers to enter into sub-processing agreements that cater for the processing of data relating to multiple customers. Acting as a processor pursuant to controller-processor
model clauses is therefore unlikely to be a practical solution for most providers and does not take account of the challenges of managing sub-contractor relationships.

Currently, some providers offer regionalised services, eliminating or reducing the need for cross-border transfer of data to a Third Country. However, such a protective approach, which hampers the ability of providers to use resources in other jurisdictions and leads to increased costs for the users, is not likely to be sustainable in the long-term.

We welcome the Commission's proposal (as articulated in its Communication of November 2010) to clarify and improve the Commission's procedure for determining that a third country provides adequate protection for personal data. Findings of adequacy are a simple mechanism for data controllers to ensure that international transfers of personal data are lawful and could, if the number of adequate jurisdictions increased, be of benefit to providers and their customers. A framework which encourages adequacy findings in respect of particular sectors or to particular categories of data importer in a jurisdiction may also be of assistance. This could include, for example, data importers that are subject to certain codes of practice or self-regulatory initiatives (see below in relation to "Data Security").

Data Security
Cloud computing provides both advantages and disadvantages. Due to specialisation and economies of scale, providers can offer security and back-up capabilities superior to those a company might provide for itself, depending on the extent of the customer's IT resources and budget. Additionally the geographical distribution of the cloud's hardware can allow for safer and more secure back-up solutions.

A disadvantage stems from the fact that physical (rather than logical) access to data is complicated by the abstraction layer introduced by virtualisation. This makes the physical reclamation of data an intractable problem given that it may be spread across multiple items of hardware and may also be stored in a proprietary data format. Where access to data is contingent on the provision of services by the provider, issues with access to the data may arise in cases of force majeure, insolvency of a provider, or more commonly, termination of the agreement or disputes between the provider and the customer.

Data controllers have obligations with regard to data security under the EU Data Protection Directive, and both data controllers (at law) and data processors (generally, under contract) must take organisational and technical measures to prevent unauthorised or unlawful processing and accidental loss, destruction or damage to the data. However, in some member states' laws, processors have direct obligations at law to ensure technical and organisational measures are implemented. Such differences in the security obligations applicable to a cloud provider, acting as a processor, can give rise to (i) uncertainty as to the required standards in relation to ensuring security and (ii) inconsistent application of security requirements across cloud solutions.

Clients recognise that cloud computing can present some unique data security issues (e.g. in relation to shared service centres, challenges associated with maintaining access controls, or implementing data segregation or other measures), but cloud computing can also offer better security solutions than when data is processed and stored at the individual data controller’s facility or in a single location by an off-site vendor. Identification of security threats, breach remediation, access controls, prevention of data leakage and implementation of best practices can in many cases be better accomplished with uniform and centralised data security management practices.

As mentioned above, companies that are subject to special security requirements will demand that their providers comply with those requirements as a matter of course. But, even when there are no specific requirements, purchasers of cloud services will demand adequate security for their data. Contractual requirements and best practices are likely to provide better and more flexible protection than specific legislated requirements that apply only to cloud services.
In this regard, we note that the Commission has expressed the view in its November 2010 Communication that self-regulatory initiatives, such as the adoption of codes of conduct, can contribute to better protection of personal data. The introduction of flexible methods of encouraging self-regulatory initiatives, including promoting codes of conduct, is potentially an attractive alternative to specific legislation concerning cloud services. However, the mechanism of self-regulation should be carefully assessed to ensure that it does not become an administratively and costly burden on customers and providers. The success of any self-regulatory regime will also require input from those stakeholders affected by self-regulation.

Processing on behalf of a data controller

There are a number of issues of particular relevance to cloud computing with regard to compliance by customers, acting as data controllers, with Article 17 of the EU Data Protection Directive, in relation to the appointment of providers acting as data processors. These include:

- difficulties in ascertaining the adequacy of technical and organisational security measures, due to the distributed computing and other systems involved;
- ensuring the right to audit, which will typically be resisted in relation to shared cloud service infrastructure, for reasons of confidentiality and security; a solution might be a third party audit based on accepted standards, e.g. the ISO27000 series or CAMM; and
- unwillingness among providers to change their standard terms and conditions, to provide warranties and undertakings in relation to security, as the business model of providers will often depend on consistent, standardised, large-scale solutions where accommodating specific requirements of one customer is either impractical or uneconomical – recent reviews by us of providers' terms and conditions shows them generally to provide only minimal guarantees regarding data security and integrity.

Strict adherence to the current requirements (e.g. physically inspecting a provider's IT infrastructure) is difficult to achieve given the operating model of cloud computing.

3.2 Are you aware of specificities in Member State data protection rules, or other legislation, that prevent you from using/providing cloud services within the EU?

Please see above in relation to specific issues with the current data protection rules. Most of these rules have a legitimate purpose, and the use of cloud services must be adjusted to this. In most cases, there are practical solutions to comply with the requirements, such as regionalised clouds (within the limits referred to above in the paragraph on “EU transfers outside the EEA”) or enhanced obligations for IT security.

In relation to other legislation:

Consumer protection/unfair terms

Providers often do not negotiate their agreements but offer a set of standard terms and conditions. They have to comply with the requirements of the laws on unfair terms in all the member states where a provider offers its services. These laws vary considerably between member states.

In the UK a number of provisions which may be found in cloud computing terms and conditions may be deemed to be unfair by the UK courts or the regulator in contracts with consumers. For example, clauses providing a unilateral right to vary the contract regardless of the consent of the other party will be likely to be found to be unfair unless such right is narrow in scope and sufficient protection is given to the consumer such that they cannot be unfairly prejudiced. Similarly,
clauses limiting the liability of the provider will also be subject to scrutiny as to whether they are unfair together with clauses enabling the provider to terminate the contract without cause on short or no notice.

In Germany the Federal Court of Justice has held that a clause in banking terms and conditions under which the bank is not liable for temporary restrictions or disruptions of access to its online-service even in case of gross negligence is invalid (XI ZR 138/00). A similar rule may apply in cloud computing contracts where a service level of under 100% is agreed on. A German court may view this as a liability disclaimer.

It should be noted that in most member states, the law on unfair terms and conditions extends to business-to-business contracts in certain circumstances.

**Intellectual property rights**

Cloud computing raises many thorny legal questions with respect to copyright.

Rights in software are regulated by the Directive on the Legal Protection of Computer Programs (91/250/EEC) and the implementing legislation in the member states. Also, the Directive on the Harmonisation of Certain Aspects of Copyright and Related Rights in the Information Society (2001/29/EC) and the relevant implementing legislation may apply. It is not entirely clear how cloud services fit into the provisions of these directives. If a cloud service user accesses software via the internet, the software is usually not physically transferred to the user's computer. If the software is actually put into the central memory of the user's computer, this will normally be the software's user interface and not the source code. There may be different situations, depending on who installs and operates the software, who has acquired it and who is then using it. A number of questions arise:

- Does a user's access to software via the internet amount to a reproduction of a computer program under article 4 (a) of directive 91/250? Is the user interface as such protected?
- Can it be regarded as the rental of the original computer program or of copies thereof under article 4 (c) of directive 91/250?
- If these provisions apply, does the exception in article 5 (1) of the directive – acts are necessary for the use of the computer program by the lawful acquirer in accordance with its intended purpose – apply? A user of cloud services does not "acquire" the software.
- Also, it is unclear whether the right of communication to the public under article 3 of directive 2001/29 is affected.

Users and providers of cloud services may find it helpful if the legislative framework were updated to provide clarity. Currently, it also remains unclear what rights are necessary for cloud-based transmission of audio and visual content, as copyright law has not kept up with the rapid development of the cloud. To alleviate some of this uncertainty, in negotiating with providers, companies will want to be specific about their ownership rights in IP in the cloud.

Further, there are concerns for providers on their potential liability for users putting infringing content into their cloud. The extent to which injunctive relief for IP infringement (under Article 11 Enforcement of IP Rights Directive; Directive 2004/48/EC) may be granted against innocent intermediaries has recently been considered by the ECJ's decision in the L'Oreal v eBay case (C 324/09). Member states' laws as to whether an intermediary service provider can be considered jointly liable for an IP infringement by a user of the service are not harmonised. A uniform approach and some clarity in this regard would be desirable.
Competition law
Parties to cloud computing agreements must comply with EU competition law and the competition laws of relevant member states. Broadly, these rules prohibit agreements and practices which restrict competition and prohibit dominant companies from abusing their market positions. While the full impact of competition law on cloud relationships may not become apparent until cloud computing models are better established, some key issues relevant to providers and customers negotiating cloud agreements, particularly with regard to competition in "after-markets", are evident.

Telecoms regulatory law
Cloud services may be regarded as telecommunications services under the relevant telecommunications laws of the member states. For example, in some member states the notification obligations may apply to Communication as a Service (CaaS) offerings and combined cloud computing and internet access offerings. Providers of such services may also have to comply with information and accounting obligations towards their customers. In addition, there may be obligations for technical measures to ensure data security.

Risk Management
A shift to cloud computing, much like any decision to outsource business functions, has an impact on risk management of companies. However, in the case of cloud computing the impact may be exacerbated by the distributed nature of the services. On the other hand the cloud offers great opportunities to achieve higher standards of protection and risk mitigation that any one company can achieve on its own. This is a matter of carefully checking the "design" of the cloud (by due diligence or otherwise) and discussing the risks with the providers. Some providers already offer ring-fenced clouds for various different products and data flows, thus protecting data and mitigating risk. Providers can and should use risk mitigation to their advantage and position the security measures offered by them as a way to differentiate themselves from the competition.

Tax
The tax rules of individual member states would need to be checked to see if there are requirements relating to the location of computerised tax records. Some jurisdictions have special rules (such as Germany), whilst others do not (such as the UK and Luxembourg).

In Germany, there are additional legal requirements for users putting tax relevant bookkeeping records into a cloud where servers are based outside Germany. Section 146 of the German Tax Code (Abgabenordnung, AO) normally requires all businesses in Germany to keep all tax relevant bookkeeping records within Germany. The tax authorities may grant an exception for electronic bookkeeping abroad if (i) the business informs the authority about the location of the data processing system and the name and address of a third party provider, (ii) the business complies with other obligations for bookkeeping, (iii) the authority's full access to the data on the processing system is guaranteed, and (iv) there is no negative impact on the taxation. With cloud computing, it may be hard to locate exactly where data is stored. In effect, German tax relevant bookkeeping records should in principle only be put into regionalised clouds or clouds where data can at least be located somewhere. Tax authorities may also grant alleviation from those requirements at their discretion.

In the UK, Belgium, the Netherlands and Luxembourg there are no special rules requiring those tax records which are stored electronically to be stored locally. For instance, in the UK, generally it is more important that the taxpayer can covert any computerised data and computerised tax records into a satisfactory, legible form on the request of the tax authorities. In Belgium the CBN (Belgian commission for accounting standards) has stated in its Opinion 2010/14 of 24 September 2010 that it allows tax records to be kept on a computer abroad provided the method of archiving allows full access from Belgium.
However, electronic VAT records may be treated differently. Some member states (e.g. the UK, and Belgium) have special rules for storing VAT invoices electronically, including where these may be stored. The Netherlands requires that on line access is guaranteed and that, in the case of electronic invoices which are stored in another member state, the tax authorities have a right to access, download and use the invoices electronically. Article 245 of the VAT Directive (2006/112/EG) allows member states to require taxable persons established in their territory to store VAT invoices within that territory, when the storage is not by electronic means guaranteeing full on-line access to the data concerned.

Regulatory requirements for financial institutions and insurance companies
Member states have enacted the Capital Requirements Directive and the Markets in Financial Instruments Directive in regulatory instruments that require financial institutions to have in place secure and effective senior management and internal systems and controls when outsourcing essential activities and processes. These equally apply to outsourcing through cloud computing and mean a financial institution must not undertake a significant outsourcing without carefully selecting and monitoring the provider, and agreeing a detailed system of contractual controls to ensure the continuity of service. Therefore, before public cloud computing is used widely, providers may need to look at providing specifically tailored offerings to the financial services sector. Until financial institutions are comfortable that a public cloud service offering will meet the financial institution's regulatory requirements, private clouds or clouds with a number of selected users with similar needs may be more appropriate.

Hosting health data
In France, the provision of health data hosting services, whether via cloud or standard facilities, requires the provider to obtain the prior approval of the Ministry of Health. Such approval is granted for three years only, on the basis of recommendations issued by the French data protection authority (the CNIL) and a specific approval committee. To get such authorisation, the provider must comply with extremely narrow conditions in terms of data security, confidentiality and effective exercise of patients' rights in their data. This specific requirement needs to be spotted at an early stage both by the provider and the potential customer, as it may impact the calendar of a contemplated project.

Professional confidentiality obligations
Some professionals such as lawyers, auditors, tax advisers, doctors, dentists etc. are obliged by law and/or rules of professional conduct to keep client information confidential, and may even be criminally liable in case of breach of such obligations (see e.g. section 203 of the German Criminal Code, Strafgesetzbuch). If such professionals wish to use cloud services for client information they must ensure the provider offers sufficient protection to ensure client confidentiality. Even then, it is not certain whether this is sufficient to prevent criminal liability. Obtaining consent from clients/patients etc. may be advisable.

3.3 From your perspective, would it be useful if model Service Level Agreements or End User Agreements existed for cloud services so that certain basic terms and conditions could easily be incorporated into the contractual agreements? If no, why not? If yes, further thoughts about how this might/should work?

Such model agreements could be helpful in practice if they are carefully drafted, ensure a fair balance between users' and providers' rights and obligations, are clear and user-friendly in language and structure and cover all relevant aspects. The model agreements must ensure sufficient flexibility to be useful for different types of services as well as different user needs. Practitioners must be involved in the drafting process.

However, in practice model SLAs will only work if there is a sufficient differentiation between the various types of providers and customers. This will require variants ranging from agreements with individual or consumer customers all the way through to model SLAs for large enterprises. Including a range of model SLA's recognises that large customers have significant buying power and are able to achieve higher SLA's and stronger contractual commitments from the
provider. Further, while model SLAs would be a useful guide there should be an acknowledgement that (at least where the parties have equal bargaining power, for example where the customer is a large enterprise) the provider and the customer contractual freedom to agree alternative SLAs.

With respect to end user agreements, we take the view that over time the cloud computing market will become increasingly competitive, and disrupters will emerge within providers which challenge the status-quo in terms of contractual commitments provided to customers. As cloud computing becomes more common and competition for customers at the enterprise level heats up, concessions will be required in order to remain competitive.

Experience with model agreements used in the public sector for the procurement of IT services in Germany (Ergänzende Vertragsbedingungen für die Beschaffung von IT-Leistungen, EVB-IT) has shown that the involvement of industry associations (e.g. BITKOM) at an early stage helps to establish a legal framework that is accepted as market standard. In contrast, providers sometimes fear unbalanced terms and conditions with an increased liability exposure where terms are unilaterally dictated. For example, our impression is that providers were more reluctant to participate in tenders based on the terms for development of IT systems (which were published by the Federal Ministry of the Interior in 2007 before consent with the industry could be reached) than in tenders based on the terms for sale of IT systems (which were developed in accordance with BITKOM).

In summary, we believe that creating standard form terms may not be necessary.

4. **Embracing Interoperability**

No response.

5. **Public sector clouds**

No response.

6. **Future research and innovation programmes**

No response.

7. **Global solutions for global problems**

7.1 What are the most important Cloud Computing problems that have to be discussed at global level? Please list and explain.

As we have stated, many of the challenges faced by cloud computing are not new challenges. They may just be magnified by the potential size and reach of cloud computing capabilities or by the fact that the cloud is "new". We believe that the most important issues which need to be discussed so that existing legislation can be adapted and applied in a meaningful and clear way are:

- Data security
- Jurisdictional risks and governing law
- Harmonising data protection obligations.
7.2 *Which would be the right fora/approaches to tackle them? Please expand.*

We believe that open discussions between legislators, users and providers and other interested parties may work best. Some issues may require limited adaptations of existing laws, others can be solved by the industry and the users themselves. All measures should enable the cloud to expand, not limit its further development. We should not create too many rules specifically for the cloud since such rules cannot keep pace with the development of the cloud and will therefore soon become outdated and ineffective, or worse, unintentionally restrictive.
Appendix 1

About Allen & Overy

Allen & Overy LLP is an international legal practice with about 4,750 staff, including about 480 partners, working in 38 major cities in 26 jurisdictions worldwide. Its European offices are in Amsterdam, Antwerp, Athens (representative office), Bratislava, Brussels, Bucharest (associated office), Budapest, Düsseldorf, Frankfurt, Hamburg, London, Luxembourg, Madrid, Mannheim, Milan, Munich, Paris, Prague, Rome and Warsaw. A&O's clients include banks, corporations, sovereign states and individuals.

Allen & Overy has one of the most respected, world-wide commercial practices in the global marketplace. We have expertise in all types of commercial contracts including contracts covering services, outsourcing, licensing, R&D, distribution, marketing, manufacturing, supply, maintenance and support, and online terms and conditions. We also advise on non-contractual commercial issues such as data protection, freedom of information, document retention policies, e-commerce and sales law.

We act for leading technology suppliers and international corporate customers from a wide range of sectors on the procurement and distribution of major technology and e-commerce systems and services. We have extensive experience of advising clients on all aspects of software licences, hardware procurement, service supply arrangements, software and e-commerce development contracts, online services, cloud computing, data protection, encryption policies and related regulatory issues. We are also widely involved in formulating and responding to policy developments for many leading companies.

Our success is built on our ability to combine the technical skills of our professionals with the business needs of our clients. We pride ourselves on the calibre of our team, the quality of our legal expertise and our ability to deliver projects that are robustly drafted.

Highlights of our recent cloud computing experience include acting for:

- one of the largest pharmaceutical companies in the world on a global 'cloud computing' outsourcing transaction with Microsoft.
- a leading telecommunications organisation on a contract to provide global data centre and SAP infrastructure services to healthcare, lifestyle and lighting giant Philips Electronics. This was one of the biggest outsourcing deals in the market in 2009, and innovative in that it involved the adoption of a SAP SaaS model, utilising a private cloud.
- a leading telecommunications organisation on a bidding procedure to outsource virtually all IT and telecommunication processes of E.on AG.
- a global online retailer on strategic copyright issues across the European Union in relation to its recently launched storage solution for audio visual files including music, videos and photos.
Appendix 2

Your Allen & Overy Contacts

Filip van Elsen  
Partner, Antwerp  
Contact  
Tel: +32 3 287 73 27  
filip.vanelsen@allenovery.com

Jim Ford  
Partner – Corporate  
UK – London  
Contact  
Tel: +44 20 3088 4797  
jim.ford@allenovery.com

Herald Jongen  
Partner, Amsterdam  
Contact  
Tel: +31 20 674 1614  
herald.jongen@allenovery.com

Ahmed Baladi  
Partner, Paris  
Contact  
Tel: +33140065342  
ahmed.baladi@allenovery.com

Nadine Herrmann  
Partner, Hamburg  
Contact  
Tel: +49 40 82221 2129  
nadine.herrmann@allenovery.com