

## Our response to the EC Consultation on Cloud Computing

### Clouds for users

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?

-

2. Please comment.

-

3. 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?

Yes

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

-

5. Please comment.

Jurisdiction should be applied in light of the country of origin of the cloud provider, regardless of where the customer's data is stored, provided that the provider has its main operation in this country and provided that the country has a reasonable level of customer protection. The perception that data in the cloud can be anywhere leads to confusion with regard to how the law should be applied. By this mechanism, both clients and cloud providers will know the legal framework surrounding their relationship.

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

No

7. Why?

The issue of liability poses a challenge to industry. Currently in multi tenancy arrangements, single faults can impact multiple contracts creating a snowball

effect of liabilities - therefore suppliers are particularly reluctant to offer indemnities, relax limits of liability and agree to one-to-one governance and dispute resolution processes. This creates a huge degree of uncertainty for customers of a cloud offering, which represents one of the fundamental limitations of the typical commercial arrangements associated with cloud computing.

This is likely to deter many customers from engaging a cloud supplier, particularly within public sector bodies, which are more traditionally risk averse.

One important area of liability surrounds data losses and data breaches. Most limitation of liability provisions in cloud computing contracts include both a financial cap on liability and an exclusion of indirect and consequential losses. From the customer's perspective the financial cap needs to be sufficiently high so that the costs of re-inputting data manually will be recoverable.

### Legislative Framework

1. and 2.

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?

Yes.

Where a cloud computing service involves some processing of personal data, then the service has to meet the requirements of the Data Protection Directive (95/46/EC) if the customer is established in a EU Member State, or the data is processed in an EU Member State. Although all of the Directive is of relevance, the provisions that seem to cause most tension with cloud computing are:

- distinctions between controllers and processors;
- restrictions on data transfers; and
- extensive administrative and controlling obligations of data controllers.

Compliance difficulties are magnified due to the fact that there can be wide differences between implementation of the Directive in the 27 EU Member States, so solutions that work in one country may not work elsewhere. Greater harmonisation of procedural obligations and notions introduced under Directive 95/46/EC would therefore be welcome. Another essential point is that data must be deleted by the cloud computing providers once a user no longer wishes to use the service. This can lead to problems, particularly in connection with backups created by providers that contain data belonging

to a number of customers where targeted deletion of individual data items proves financially unreasonable or technically inappropriate. Of course, irrespective of the costs incurred this right to delete for the data subjects should be reaffirmed and strengthened. However, it must be adapted to the technology reality.

3. and 4.

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?

Yes.

We have gathered information from 13 EU countries where Bird & Bird has offices, namely: Belgium, Czech Republic, Finland, France, Germany, Hungary, Italy, Netherlands, Poland, Slovakia, Spain, Sweden and the UK. For most of those countries, we are not aware of any data protection rules or legislation preventing the use/provision of cloud computing services. However, the following observations must be made:

- Under Czech law, the service provider would most likely be considered a data processor but that would depend largely on the nature of services;
- Under Finnish and Swedish law, especially concerning public entities, there may be provisions regarding security restrictions which could prevent the provision/use of cloud services;
- In France, controllers need to specify the exact third countries to which data are to be transferred in order to obtain an authorisation from the French Data Protection Authority. Note that a report from the National Assembly dated 22 June 2011 (“Rapport d’information sur les droits de l’individu dans la révolution numérique”) suggests drafting new legislation, where cloud computing solutions located outside the EU would be barred from processing sensitive data. Presently, there is no indication that this proposal will be turned into law;
- Under German law, cloud providers are seen as data processors. Both the strict, impracticable German requirements for data processing agreements and the particular view of German data protection authorities on Safe Harbor are major issues for cloud computing. There are even opinions of German data protection authorities that cloud computing, in particular in non-EU/EEA-clouds are not legally possible at all;
- The Italian Data Protection Authority issued a general Resolution - published in the Official Gazette No. 153 of 4 July 2011 - outlining a new principle for the appointment of data processors by companies which outsource personal data to external agencies. Under the Resolution, companies which outsource work but ‘maintain operational control’ must formally nominate the agencies as ‘data processors’;
- Under the Dutch Data Protection Act, controllers need to specify the exact third countries to which data are to be transferred in order to obtain a permit;
- Under Slovakian law, state authorities may have issues with using cloud computing services located in other countries with regards to classified information;
- In Spain, in most cases, providers of cloud computing solutions will be defined as ‘data processors’.

5. and 6.

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?

No.

In order to gain the most out of the market, there is a strong argument for allowing suppliers to decide their own terms and allow them to compete on that basis. However this relies on customers evaluating terms and conditions as part of their solution evaluation and not as part of a separate legal workstream. In addition, it is difficult to see how a useful standard set of SLAs could be produced, when there are so many different types of cloud offering and definitions of those services.

## Embracing interoperability

1. Please describe interoperability or (data) portability issues you have encountered when using/providing cloud services or are otherwise aware of.

We see interoperability as a significant concern for the market. In order to be viable, compatibility between different computer systems is important. This in itself facilitates ease of switching suppliers. In order to further facilitate easy movement between suppliers, shared values, or a set of guidance/standards would be useful in determining what format such data will be recoverable.

2. Which existing or emerging standards support interoperability across and portability of data (from one cloud to another)? *Please list and describe.*

-

3. Which are the most important standards that are currently missing but which you feel are necessary to ensure interoperability and portability? *Please describe in detail the aspects they should cover.*

-

## Public sector clouds

1. What can the public sector do as a cloud user to support the emergence of best practices?

The public sector can help in the following ways:

- Create an open market place by increasing transparency;
- Ensure that procurements are run fairly and simply, assisting the creation of a level playing field, encouraging both traditional, non-traditional large and SME suppliers to take part;
- Continue with Government-wide projects such as G-Cloud;
- Establishment of best practice for Cloud data security management including data access, physical location security, backup encryption and physical security;
- Establishment of best practice guidance for Cloud service provision for availability and performance;
- Reorganise business processes to make best use of cloud services;
- Developing a greater understanding of risk and tolerances across Government; and
- Educate consumers across other sectors (e.g. energy, finance and other sectors).

2. Please elaborate in particular on public procurement of cloud services.

Standards are vital to encourage the public sector to adopt cloud technologies more widely. EU-approved procurement models for Healthcare/Public Sector/Specialised clouds are needed. Existing procurement and management controls often prevent the adoption of innovative solutions and steer procurement to the traditional bespoke responses. This model must change in order to encourage the market to grow. There is the possibility of creating a hybrid of a dynamic purchasing system and a framework that allows suppliers who meet set criteria to enter the system (likely a comparative online catalogue) at any time rather than when a procurement is run (i.e. the market is always open). Customers could then call off services based on evaluation between offerings that are on the catalogue. This will encourage commodity buying. This means use of different procurement models and approaches. Many of these are not well developed under EU.

3. In particular, can the deployment of eGovernment and eScience infrastructures by the public sector act as an example for other sectors?

-

4. Please list Member State initiatives in the area of Cloud Computing that you are aware of.

Government's shift to a framework providing for the adoption of cloud services across government (previously known as G-cloud)

5. How can Member States best cooperate to create interoperable solutions and shared best practices?

-

## Future Research and Innovation programmes

1. Which are the most important technical aspects of cloud computing that researchers are currently working on? Please explain the importance of each concrete example.

-

2. Beyond these, do you see technical problems/limitations of current cloud service offerings that will require further research in the coming years?

-

3. Please elaborate.

-

4. Should public R&I funding be used to establish prototypes of new cloud infrastructures?

No

## Global solutions for global problems

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

As this is a global technology, it is important that problems are addressed at a global level and that there is agreement between providers on the best way forward. We see the following as important issues:

- Data Protection - as already set out, data protections need to be harmonised;
- Interoperability standards- as already set out in the response;
- Consumer Protection - work is needed on supplier standard terms of business to ensure that consumers are adequately protected. At present, they are very one-sided.
- Enforcement of Terms
- Export controls - when is an export taking place? Do companies know the path of data? Is technology sufficiently sophisticated to allow for this degree of Regulation? If not, some suppliers/customers may become unstuck.

- Security - this needs to be of a sufficient level to encourage take up by commercial organisations that hold sensitive data, without this, the market will always be limited.
- Who is the responsible regulator? As discussed, cloud service providers may find themselves in a situation whereby they are forced to consider a number of different jurisdictions' regulatory requirements. These should be streamlined or consolidated into one organisation.

2. Which would be the right fora/approaches to tackle them? *Please expand.*

-

## Contacts



**Roger Bickerstaff**  
Partner

T: +44 (0)20 7415 6000  
roger.bickerstaff@twobirds.com



**Fabian Niemann**  
Partner

T: +49 (0)69 74222 6000  
fabian.niemann@twobirds.com

## Contributors

Tessa Finlayson, Gabriel Voisin, Barry I Jennings, Paul McMahon

The content of this update is of general interest and is not intended to apply to specific circumstances. The content should not therefore, be regarded as constituting legal advice and should not be relied on as such. In relation to any particular problem which they may have readers are advised to seek specific advice. Further, the law may have changed since first publication and the reader is cautioned accordingly.

# twobirds.com

Abu Dhabi & Beijing & Bratislava & Brussels & Budapest & Düsseldorf & Frankfurt & The Hague & Hamburg & Helsinki & Hong Kong & London & Lyon & Madrid & Milan & Munich & Paris & Prague & Rome & Shanghai & Singapore & Stockholm & Warsaw

Bird & Bird LLP is a limited liability partnership, registered in England and Wales with registered number OC340318 and is regulated by the Solicitors Regulation Authority. Its registered office and principal place of business is at 15 Fetter Lane, London EC4A 1JP.  
Bird & Bird is an international legal practice comprising Bird & Bird LLP and its affiliated and associated businesses and has offices in the locations listed on our web site: twobirds.com.  
A list of members of Bird & Bird LLP, and of any non-members who are designated as partners and of their respective professional qualifications, is open to inspection at the above address.