

## Cloud computing Ts and Cs – News from Europe

*Three developments of use in and beyond Europe, the first providing a great resource for negotiating cloud computing contracts:*

### **Cloud Legal Project's work on negotiating cloud contracts**

Earlier work by the Cloud Legal Project is outlined in our article, *Cloud computing contracts often have poor terms: survey results*.<sup>1</sup> Now, as well as producing a helpful summary on UK G-Cloud contracts,<sup>2</sup> the Project has released a useful paper on how corporate customers are getting on with negotiating cloud contracts with suppliers. It's called, *Negotiating Cloud Contracts – Looking at Clouds from Both Sides Now*.<sup>3</sup>

The authors make the point that the terms negotiated by large corporates may filter down from changes in the large deals<sup>4</sup>. The information, based on their research, will be handy in negotiating with suppliers; benchmarking against what's happening with others is valuable. And suppliers will find out what other providers are up to in this space. What's seen as important by big customers? On what points will suppliers negotiate? Where will they hold firm? Where will suppliers insist of using the standard delivery model (a benefit of cloud computing) instead of allowing tailored services? What should business customers do about click-accept terms? Where do system integrators fit?

The Cloud Legal Project rates the following areas as the most negotiated:

1. Limitation of liability and remedies (particularly as to data integrity and DR);
2. Service levels including availability;
3. Security and privacy;
4. Lock-in and exit, including term, termination rights and return of data on exit (Wigley & Company rates this as important);
5. Provider's ability to change service features unilaterally; and
6. IP

### **European Commission**

On 27 September, the European Commission released its paper, *Unleashing the Potential of Cloud Computing in Europe*. With predicted impact in Europe on GDP of 957bn euro and 3.8m jobs by 2020, the Commission is looking to get the right framework to encourage strong European uptake and wins. This includes:

- standards for interoperability (not only is that an issue around service standards and protecting customers' ability to move from poor services, it's also an anti-trust issue, as we've noted in our paper, *Cloud Computing: regulatory/anti-trust risks and solutions*.<sup>5</sup>
- standard cloud computing terms and conditions meeting needs such as in relation to predictability, interoperability, data protection, fairness between suppliers and customers including SMEs, larger corporates consumers and public sector.

Broadly, there will be industry-based development and consultation toward developing optional terms. So, detailed regulatory requirements will be held back for the present, although consumer regulation and data protection may see a push. The less regulated approach could change if the voluntary approach doesn't work.

The Commission and industry could develop terms and standards of use outside the EU over the next year or two.

October 2012

Cloud computing Ts and Cs  
– News from Europe

**Data Protection, Privacy and Security**

The UK's data protection regulator, the Information Commissioner's Office (ICO) has produced useful Guidance on the use of Cloud Computing. OECD-based privacy regulation tends to have requirements reflecting what would be good industry practice in relation to security and data protection. The effect of other law is often similar. For a summary of legal requirements see our article, *Security in the Cloud*.<sup>6</sup>

A key focus of the ICO guidance is that organisations remain responsible for how their data is looked after, even after passing it to a cloud computing provider. The guidance includes these tips:<sup>7</sup>

- Seek assurances on how your data will be kept safe. How secure is the cloud network, and what systems are in place to stop someone hacking in or disrupting your access to the data?
- Think about the physical security of the cloud provider. Your data will be stored on a server in a data centre, which needs to have sufficient security in place.
- Have a written contract in place with the cloud provider. This is a legal requirement, and means the cloud provider will not be able to change the terms of the service without your agreement.
- Put a policy in place to make clear the expectations you have of the cloud provider. This is key where services are funded through adverts targeted at your customers: if they're using personal data and you haven't asked your customers' permission, you're breaking data protection law.
- Don't forget that transferring data internationally brings a number of obligations – that includes using cloud storage based abroad.

1. <http://www.wigleylaw.com/assets/pdfs/2011/cloud-computing-contracts-often-have-poor-terms-su.pdf>
2. UK G-Cloud v1 and the impact on cloud Contracts, W Kuan Hon, C Millard and I Walden (QMC Legal Studies Research Paper 115/2012)
3. W Kuan Hon, C Millard and I Walden (QMC Legal Studies Research Paper 117/2012)
4. and filter up from regulatory changes in relation to consumers.
5. <http://www.wigleylaw.com/assets/pdfs/2010/cloud-computing-regulatory-anti-trust-risks-and-so.pdf>
6. <http://wigleylaw.com/assets/pdfs/2010/security-in-the-cloud.pdf>
7. Quoting the ICO's press release of 27 September 2012