McCann FitzGerald

Cloud Computing: Key Legal Issues

FACTSHEET

Cloud computing is a relatively new technology which is still evolving. It has been hailed as providing the perfect solution for managing the ever-increasing volume of data which companies are producing nowadays. This is due to the significant cost and storage savings it can provide. As with many new technologies, however, there has been a great deal of trepidation about cloud computing. As a result, businesses have been slow to embrace the benefits which it has to offer. For example, a recent study showed that 35% of businesses in the UK are using cloud services as compared with 58% in the US.

INSTITUTE OF DIRECTORS IN IRELAND

This factsheet was produced by the Institute of Directors in association with McCann FitzGerald for use in Ireland. McCann FitzGerald is one of Ireland's premier law firms, providing a full range of legal services to many of Ireland's leading businesses. Clients include international organisations, major domestic concerns, emerging Irish companies and clients in the State and semi-State sectors.

www.mccannfitzgerald.ie

What is Cloud Computing?

The main types of cloud computing are as follows:

- Software as a Service (SaaS) (*eg* Hotmail, Gmail): in this model the provider hosts commercially available software which is made available to the customer over the internet.
- Platform as a Service (PaaS) (*eg* Salesforce): in this model the customer rents virtualised servers and related services for running existing applications or for developing and testing new ones.
- Infrastructure as a Service (IaaS) (*eg* Amazon s3 Storage): in this model the customer outsources its equipment requirements (*eg* storage, hardware, servers, networking components, *etc*) to the cloud service provider.

Risks and Benefits

There are a number of benefits associated with cloud computing. In the first instance, as the services are delivered over a network they are accessible through any device or location. This facilitates remote working arrangements and is consistent with the increasingly globalised nature of doing business. Cloud services also confer a number of commercial benefits. For example, they benefit from rapid elasticity or scalability as the resources required to deliver the services can be easily expanded or reduced to meet the customer's requirements. Cloud based services also tend to operate as a measured service meaning that payment is based on a particular number of users rather than paying a once-off licence fee which includes a premium for unlimited use. A further benefit is that of on-demand self-service. This means that the customer can use or adjust the services without engaging customer service which either eliminates or significantly reduces support and maintenance costs.

Of course there are a number of very significant risks associated with cloud computing. The main risk arises from the loss of control over data. There may also be a lack of visibility over where data is actually being processed. Often the cloud provider entering the contract will be based in a particular jurisdiction but will use servers or sub-contractors all over the world to host the data. Concerns over security are also a significant issue. Risks include unauthorised access by other users of service or service provider personnel. The system may also be vulnerable to external cyber-attacks. Customers may further be concerned about the ability to recover their data if the supplier becomes insolvent and a further issue is lack of portability (*ie* the cloud provider stores data in a format which is not readily transferable back to the customer or to a replacement service provider).

Contractual Issues

One of the difficulties faced by customers is that many cloud providers insist on their own standard form terms and conditions. Not surprisingly, these are usually very one-sided in favour of the cloud provider and the scope for negotiation by the customer is limited or non-existent. Fortunately this position is beginning to change (though is still a long way from being eradicated). A number of the large cloud providers such as Google and Microsoft have been persuaded to change their terms and conditions by data protection regulators to ensure that data remains adequately protected. Also, public bodies subject to the public procurement rules are increasingly issuing contracts which cater for cloud solutions as part of their invitation to tender for information technology services.

Regardless of whether the contract is based on the supplier or the customer's template agreement, there are a number of contractual provisions which one would expect (or should not reasonably expect) to see in a cloud computing contract. These are discussed below.

- **Acceptance Testing:** as the cloud solution is unlikely to have been customised or developed specifically for the customer, any acceptance testing provisions will be more limited than would be in the case of a more traditional software development contract. The customer may still wish, however, to provide for some degree of end-to-end testing before going live on the system.

- **Warranties:** the warranties should be broadly similar to those which would appear in any IT services agreement. These include warranties that: (i) the solution will perform in accordance with specifications (usually the supplier's standard/published specifications rather than any particular specifications agreed with the customer); (ii) that the cloud provider will provide the services with due skill care and diligence using appropriately skilled and qualified personnel; and (iii) the supplier will use all reasonable endeavours, in accordance with best industry practice to prevent the introduction of computer viruses or other malware into the cloud solution.

- **Ownership of Data/Intellectual Property:** the contract should very clearly provide that all data and materials provided by the customer (and all intellectual property rights in such material) remain vested in the customer. The intellectual property rights in the solution will remain vested in the cloud provider.

- **Licensing:** the customer will be granted a limited licence to access and use the solution. The customer will not receive a physical copy of software and nothing will be installed on the customer's equipment. As such, provisions around delivery or installation of software will not be relevant.

- **Indemnities:** the cloud provider should indemnify the customer against any claims that the solution infringes the intellectual property rights of any third party. As the cloud provider owns the intellectual property rights in the system, it is appropriate that liability for any infringement claims are allocated to the supplier and not the customer. This would be the usual approach in any software licensing arrangement. The customer should also seek an indemnity for breach of the data protection and confidentiality provisions in the contract. This would be less common in more traditional forms of IT contracts but is appropriate here given the risks associated with the customer entrusting its data to the cloud provider.
- **Limitation of Liability:** the supplier will seek to limit its liability under the contract (usually by reference to the amount of fees paid by the customer). It would be important, however, to carve-out recovery under indemnities (*ie* intellectual property claims/data protection breaches) so that liability is unlimited or is at least capped at a higher level than the general limitation which applies.
- **Disaster Recovery:** the contract should clearly provide that the cloud provider is responsible for ensuring that appropriate disaster recovery measures are in place. Usually a disaster recovery plan will be agreed between the parties and annexed to the contract. The contract should also provide for regular testing (eg at six-monthly intervals) of the agreed disaster recovery processes to ensure that they work.
- **Service Levels/Service Credits:** the effectiveness of the cloud service will depend heavily on the standard of service provided by the supplier. As such, it is appropriate to include a service level agreement in the contract containing service levels (*eg* relating to the availability of system and response/resolution times for the correction of any defects arising) and ideally service credits which are payable when the required service levels are not met.
- **Ring-Fencing/Recovery of Data:** the contract should require the cloud provider to ensure that the customer's data is fully segregated from data belonging to other customers of the cloud provider and the provider's own data. The supplier should also be obliged to ensure that the data is easily recoverable by the customer at any time during the term of the contract or on termination and in a format which can be easily transferred to the customer or to a replacement service provider.
- **Data Protection:** the recommended provisions are discussed in more detail below. One of the key requirements will be to ensure that the customer has full visibility at all times of the location where data is being processed.
- **Escrow:** unlike more traditional forms of software licensing, escrow is unlikely to be relevant in a cloud solution. If the supplier becomes insolvent or fails to maintain the solution in accordance with its support obligations, the key concern for the customer will be getting its data back rather than getting access to the source code to run the system itself which would not be appropriate in a cloud based model.

Data Protection Issues

The general principles under Data Protection Acts 1988 and 2003 ("**DPA**") apply. A key point is that the customer remains the data controller and the cloud provider acts as a data processor processing personal data on the customer's behalf. As

the customer is established in Ireland, Irish data protection law will apply regardless of where the cloud provider is located. The risk, of course, is that as data controller, the customer remains primarily liable for data protection breaches even if such breaches are caused by the cloud provider.

The Data Protection Commissioner ("**DPC**") has issued guidance on "Data Protection in the Cloud" which is based primarily on the Article 29 Working Party Opinion 5/2012. The DPC identifies the main issues as being data security and the location of the data. As a minimum, a written contract (a short-form data processor agreement) must be put in place between the customer and the cloud provider whereby the cloud provider agrees to: (i) process the data solely in accordance with the instructions of the customer; and (ii) to implement and maintain appropriate security measures in accordance with the requirements of the DPA.

The DPC also recommends including the following specific protections:

- Provide for continued access to data by way of appropriate back-up/disaster recovery measures;
- Ensure that appropriate steps are taken to prevent unauthorised access (*eg* from external hacking, cloud provider personnel or other users of the cloud service);
- Ensure that the customer has adequate oversight of the cloud provider and sub-contractors (*ie* full visibility of where data is being processed and right of audit);
- Agreed procedures in the event of data breach – the cloud provider should be required to report security breaches immediately so that the customer can comply with its notification obligations under the Personal Data Security Breach Code of Practice and the Electronic Privacy Regulations (SI 336/2011) (as relevant); and
- Data portability: the customer should have the right to remove or transfer data at any time on request.

With regard to the right of audit in respect of the cloud provider and its sub-contractors, the DPC recognises that it would not be practicable in a multi-tenanted cloud environment for each customer to have a direct right of audit. As such, the DPC indicates that third party certification to international standards would be acceptable in such circumstances.

The location of the data is also of key importance from a data protection compliance perspective. If the data is processed within the EEA or a country which is deemed to have adequate protection (*ie* EU, Iceland, Liechtenstein, Norway, Switzerland, Canada (to limited extent), Guernsey, Argentina, Isle of Man, Faroe Islands, Jersey, Andorra , Israel, New Zealand and Uruguay), a Short-Form Data Processor Agreement will be required under the DPA. If the data is being processed outside the EEA in a country which does not have adequate protection, it will also be necessary for the customer to satisfy one of the exceptions to the prohibition on such transfers. The main exceptions likely to be relevant here are that the cloud provider has signed up to the Safe Harbor principles (though this will only be relevant for US entities) or that the customer and cloud provider have entered into a model contract (controller to processor) in the form approved by the European Commission. It will also be important to ensure that one of the exceptions to the prohibition is satisfied in respect of any sub-contractors located in countries which do not confer adequate protection.

Adequacy of Key Cloud Provider Terms and Conditions

It is interesting to note that the adequacy of certain key cloud provider terms and conditions has been considered by the data protection regulators in some of the Nordic countries. In Norway, the regulator initially held that the Google Apps and Microsoft 365 terms did not comply with local laws due to: (i) the loss of control over storage and access restrictions; and (ii) the fact that the terms did not satisfy local requirements in respect of data processor and transfer agreements and security. The regulator also queried whether the Safe Harbor regime still provided an appropriate basis for transfer since it predated the US Patriot Act. Less than a year later, however, the Norwegian regulator approved the Google and Microsoft terms for two municipalities. It justified the change of direction on the basis that both providers had improved their security measures. The regulator also made the approval subject to conditions being satisfied (*ie* a thorough risk and vulnerability analysis to be carried out; satisfactory data processor agreement to be concluded and enforced; the performance of regular audits; and unless the country has adequate protection, model clause contracts).

In Sweden, the data protection authority rejected the adequacy of Google Apps for use by a Swedish municipality. The reasons cited were: (i) uncertainty over how data may be mined or processed; (ii) lack of clarity around the use and location of sub-contractors; and (iii) uncertainty around deletion of data on termination. By contrast, the Swedish authority later accepted Microsoft's Windows Azure for use by a private entity. On its own website Microsoft states that it is willing to append the EU Model clauses for Office 365/ Microsoft Dynamics CRM Online. It also states that the adequacy of standard terms for these products has been approved by the data protection authorities in various countries including Ireland.

European and Other Initiatives

The European Commission issued a paper entitled: "Unleashing the Potential of Cloud Computing in Europe" in September 2012. The paper outlined a number of steps to be taken which the Commission claimed would deliver a net gain of 2.5 million new jobs in Europe and provide an annual boost of EUR 160 billion to EU GDP by 2020. The steps proposed were as follows:

- The development of model contract terms similar to the model contracts developed for data transfer purposes;
- The development of uniform standards throughout Europe to ensure greater interoperability, data portability and reversibility; and
- Establishment of a European Cloud Partnership to work on common procurement requirements for public sector with regard to cloud computing.

An expert group was established in June 2013 (Commission Decision 2013/C 174/04) to work on the common procurement requirements. On 28 October 2013, the European Commission further announced the establishment of an expert group to work on safe and fair contract terms. It is hoped that the initiative will now progress at a faster rate.

Separately, the UK Government launched its G-Cloud initiative within the last 18 months. One of the key features of this is the establishment of a cloud store where potential customers within the Government sector can browse through a panel of pre-approved cloud products and suppliers. The aims and objectives of the initiatives are as follows:

- Achievement of large scale cross-government economies of scale;
- Flexible, demand-led systems to support Government policies and strategies;

- Deployment of new technologies to deliver faster business benefits and reduce cost;
- Assist the Government in meeting environmental and sustainability targets; and
- Allow Government to procure in a way that encourages a dynamic supplier market which supports emerging suppliers.

In its first 18 months, G-Cloud has approved over 800 suppliers (83% of which are SMEs) and 7000+ services. It has also generated £44.7M in sales with 63% of all contracts awarded having been awarded to SMEs.

Closer to home, the Irish Government launched a paper on Cloud Computing Strategy in June 2012 as part of its programme for public sector reform. The aims outlined in the paper include: (i) placing cloud computing at the heart of Government ICT strategy; (ii) centralising and implementing common IT needs as a set of shared services; (iii) reducing the number of computer and data centres significantly (ie from hundreds to approximately 10 primary facilities); (iv) maximising use of external service providers and enhancing competition by establishing multi-vendor procurement frameworks; (v) setting timelines for a phased migration to cloud computing and shared services; and (vi) establishing a new ICT organisational structure and new ICT funding and governance arrangements.

Conclusion

Like it or not, cloud computing is here to stay. Whilst there are undoubtedly greater risks with cloud computing than with traditional technology solutions, it is simply a case of trying to manage those risks by ensuring that appropriate contractual protections are in place. If big names such as Microsoft and Google can be persuaded to amend their terms and conditions to ensure that data remains adequately protected, this sets a very positive example to other cloud providers. Also, if the European Commission succeeds in its aim to achieve greater standardisation in terms of security, interoperability and contract terms, this should further help to reduce the risks associated with cloud computing. The Commission will need to be mindful not to over-regulate the industry as this could stifle innovation and make the EU less attractive to cloud providers. If the Commission gets the balance right, however, this should significantly improve uptake and provide customers with the necessary degree of confidence that is currently lacking.

Further Information

Director Training

The IoD can help you refresh your skills and improve performance as a director. For information on director development courses and workshops please contact Sheila Byrne on 01 411 0010 or sbyrne@iodireland.ie

Books

Directors' Handbook

To order a copy of this publication please contact IoD Ireland on 01 411 0010

A Handbook for Directors of Regulated Financial Services Companies in Ireland

To order a copy of this publication please contact IoD Ireland on 01 411 0010

Standards for the Board

Effective Director

To order these publications please telephone +44 207 766 8866 or visit www.iod.com/bookshop

Boardroom Centre

The IoD operates the Boardroom Centre - a resource for companies seeking non-executive Directors and register for IoD members seeking directorships. For details please contact Thora Mackey on 01 411 0010 or tmackey@iodireland.ie