Cloud Computing – Legal Considerations for Data Controllers

DILLON EUSTACE

DUBLIN BOSTON NEW YORK TOKYO

CLOUD COMPUTING – LEGAL CONSIDERATIONS FOR DATA CONTROLLERS

What is cloud computing and why is it relevant?

Cloud computing can be described as technology delivered as a service made available on demand over the internet. There are effectively three types of cloud computing services: software as a service ("SaaS"), infrastructure as a service ("IaaS") and platform as a service ("PaaS"). By utilising a cloud computing service, an organisation is effectively outsourcing its IT requirements.

Online email accounts (such as Gmail or Hotmail) are everyday examples of cloud computing, users of which can access their inbox from anywhere in the world. From a business perspective, cloud computing might be used as a platform for obtaining software or storage on demand. For example, an organisation may opt to outsource its storage requirements, resulting in their data being stored on another entity's server.

Cloud computing is one of the fastest growing segments of the global IT industry with use of cloud computing services forecast to increase by 40% per annum in the coming years. It forms part of the Irish Government's vision for a "smart economy" and many of the global IT firms have invested heavily in their Irish-based cloud computing competency centres. These factors have positioned Ireland at the forefront of global developments in cloud computing.

What are the benefits of cloud computing to organisations?

The use of cloud computing services can offer benefits for organisations of all sizes, including:-

- Cost reductions

The burdensome task of maintaining IT systems can be outsourced, with organisations paying for software/hardware only as and when they are needed. This greatly reduces capital investment requirements, allowing resources to be invested elsewhere.

- Access to state of the art applications

In addition to cost savings, organisations will have the ability to utilise the most up-to-date software/hardware systems, thereby increasing efficiencies.

- Flexibility

Organisations will have access to the systems and storage they require on demand. For example, software can be made available in a very short space of time and increased storage capabilities will be available as and when they are needed, without the associated cost of having such capacity in reserve.

Data Protection and Security Issues

Despite the tangible benefits listed above, Irish entities have generally been slow to embrace cloud computing as a service. This is, no doubt, due in part to certain data protection and security issues that Data Controllers[1] are obliged to investigate.

In February, 2010 the Chief State Solicitor's Office (the "CSSO") issued a statement to Government departments warning that contracts for cloud computing services being used at the time did not address issues such as data protection, confidentiality and security at a level that would be required in the public sector. At the time this letter caused outrage in the cloud computing community – how could a Government who had publicly endorsed cloud computing overtly condemn its use by Government departments? A number of key data protection and security issues arising in this regard are considered below.

Jurisdictional Issues

Section 11(1) of the Data Protection Act, 1988 (as amended by the Data Protection (Amendment) Act, 2003) (the "Data Protection Act") provides that a Data Controller is prohibited from allowing Personal Data[2] under their control to be disseminated to a jurisdiction which does not have an adequate level of data protection, subject to the exceptions set out at section 11(4). The "adequacy" or otherwise of data protection measures will depend on many factors, including the type of data being transferred and the intended use of such data. Countries within the European Economic Area[3] are automatically deemed to have an adequate level of data protection. The EU has also approved certain other countries as having a sufficient level of data protection, including Switzerland, Canada, Argentina, Guernsey, Isle of Man, Jersey and, most recently, Israel.

[1] Defined in Section 1(1) of the Data Protection Act as a person who, either alone or with others, controls the contents and use of Personal Data.
[2] Defined in Section 1(1) of the Data Protection Act as data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the Data Controller.
[3] The 27 Member States together with Norway, Iceland and Liechtenstein.

In order to be fully compliant with the Data Protection Act, a Data Controller must have total certainty as to the jurisdictions in which the data under their control may be stored. Cloud computing as a whole appears to fly in the face of this requirement. The reality of a standardised cloud computing contract is that data could be spread across various jurisdictions, each potentially with a varying level of data protection. In fact, it may be difficult to say with any amount of certainty where data is being stored at any given time.

There are ways in which the stringent provisions of section 11(1) may be circumvented, thereby allowing the Data Controller to transfer Personal Data to non-approved jurisdictions. As mentioned above, section 11(4) contains various exemptions. For example, section 11(1) will not be breached where the consent of each data subject is obtained in respect of the data transfer. Where this is not feasible, the Data Controller may consider the following alternatives:-

- the Data Controller could utilise EU-approved "Model Contracts" which contain data protection standards equivalent to EU requirements; or

- when disseminating Personal Data to the US, the Data Controller could ensure that the US counterparty has agreed to be bound by the US "Safe Harbor" arrangement.

A more straightforward solution for Data Controllers would be to limit dissemination of data to an agreed list of EEA or approved countries. Service providers may be willing to negotiate such a term, albeit at a premium over their standard service. A Data Controller will need to ensure such a term is suitably drafted in order to meet their responsibilities under the Data Protection Act.

Data Security and Accessibility Issues

Section 2(1)(d) of the Data Protection Act provides that appropriate security measures must be taken against unauthorised access to, or unauthorised alteration, disclosure or destruction of Personal Data, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. Section 2C(1) of the Data Protection Act provides that in determining what constitutes "appropriate security measures" a Data Controller must have regard to the harm that may result from a breach of security or destruction of the data. Of particular importance is the point at which data is encrypted – will encryption occur at the organisation's premises, or will it occur once the information has entered the cloud?

By utilising the cloud platform, a Data Controller will effectively be giving up control of the security of data whilst still potentially maintaining responsibility for any breach of data security. Section 2C(3) of the Data Protection Act provides that where the processing of Personal Data is carried out by a Data Processor[4] on behalf of a Data Controller, the Data Controller is obliged to ensure that the processing is carried out solely in accordance with the contract between the Data Controller and the Data Processor and that the Data Processor provides sufficient guarantees in respect of the technical security measures and organisational measures governing the processing. The Data Controller must also ensure it has the right to audit the security measures utilised by the Data Processor.

While cloud computing undoubtedly carries a degree of security risk, its proponents may argue that data security is more likely to be breached through the theft of a laptop or the failure of an on-site storage system than through the cloud. Service providers are attempting to overcome the innate risk in the cloud through various measures. For example, some cloud services are designed to sustain the concurrent loss of data in two or more facilities. In addition, organisations that hold Sensitive Personal Data[5] or other sensitive information (i.e. intellectual property or data of a sensitive commercial nature) may avail of a "private" cloud (effectively a cloud specifically for one customer) for a greater level of security. A private cloud may not, however, fulfil all the security needs of a particular organisation and should only be used where appropriate.

In addition to the above, Data Controllers must also ensure that data is accessible at all times and kept in an intelligible form. The former requirement is of particular concern, as service providers will often indicate that the service may be interrupted for scheduled maintenance or may even be suspended for a wide variety of reasons.

The Contract

Many cloud service providers offer only a standardised "take it or leave it" service level agreement containing clauses that are heavily weighted in their own favour. In addition,

[4] Defined in Section 1(1) of the Data Protection Act as a person who processes personal data on behalf of a Data Controller but does not include an employee of a Data Controller who processes such data in the course of his employment.

[5] Defined in Section 1(1) of the Data Protection Act as any Personal Data as to: (a) the racial or ethnic origin, the political opinions or the religious or philosophical beliefs of the data subject, (b) whether the data subject is a member of a trade union, (c) the physical or mental health or condition or sexual life of the data subject, (d) the commission or alleged commission of any offence by the data subject, or (e) any proceedings for an offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings.

many cloud service providers seem oblivious to the data protection issues that the cloud raises for their clients. While negotiation is always a possibility, the effective negotiation of key terms may not be a reality for small organisations coming up against global IT heavyweights.

While initial industry reaction to the CSSO's letter was negative, that letter might have a positive long-term effect - cloud service providers must now appreciate that in order to benefit from their significant investment in cloud technologies they will need to adapt the terms of their service level agreements to suit the needs of their clients.

In any event, when considering contracting for cloud computing services, a Data Controller should pay particular attention to following contractual provisions:-

- Exemption Clauses

Standardised contracts often contain sweeping disclaimers. Some go as far to disclaim any of the normal responsibilities that a Data Processor should burden. Data Controllers should take the time to identify any such disclaimers, as it is often they who will be left carrying the mantle.

- Jurisdictional Issues

As mentioned above, Irish Data Controllers have an obligation not to disseminate data to a country that is not either in the EEA or an approved country unless: (a) the transfer benefits from an exemption under section 11(4) of the Data Protection Act, (b) the Data Controllers are utilising EU-approved "Model Contracts", or (c) their counterparty is availing of the US "Safe Harbor" arrangement. To avoid any doubt, the service level agreement should specify the country (or countries) in which data may be stored.

- Termination of the Contract

It is important to determine the rights each party have to terminate the service level agreement. Such terms are often weighted heavily in favour of the cloud service provider and can be arbitrary. Notice periods can often be short, leaving little time to make alternative arrangements. Further, the process whereby data is returned to the Data Controller on the termination of the contract should be set out in detail. In particular, the timeline and format in which this process is to be concluded should be specified.

- Deletion of Data

When the time comes for data to be deleted, the service level agreement should state unambiguously that once the customer has been returned a copy of its data, the service provider will delete all reference to such data.

Conclusions

In general, Irish organisations appear to be adopting a “wait and see” approach when it comes to cloud computing. Proponents of cloud computing may argue that the slow uptake of such services in Ireland is due to a lack of understanding of the technologies involved. However, organisations are right to be cautious - cloud computing represents a new and untested frontier in data protection and security.

The risks associated with cloud computing, while arguably no greater than those associated with maintaining an independent IT infrastructure, may prohibit some organisations (especially those who deal with Sensitive Personal Data) from acquiring such services. It may be the case that organisations will utilise the cloud solely in respect of certain areas of their operations where their obligations under the Data Protection Act are less stringent.

It is the responsibility of a Data Controller to ensure the security of the data they control. Before entering into a contract for cloud computing services, a Data Controller will need to be satisfied that the service being provided complies with their obligations under the Data Protection Act. Standardised contracts often do not meet the level of data protection Data Controllers are required to provide. The belief within the industry is that Government departments and larger organisations will have to be the ones to take the first step in terms of cloud computing usage. Once this occurs, the path will be cleared for smaller organisations to follow suit.

Advocates for cloud computing argue that EU legislation will need to be amended to facilitate the expansion of cloud computing services. As it stands, the potential of the cloud is being severely limited, particularly as a result of jurisdictional issues. They feel that appropriate arrangements can be made in the legislation for the benefit of cloud service providers and consumers alike. Whether such an amendment will materialise remains to be seen. For the moment the prime focus of the legislation is the protection of Personal Data.

Date: **May, 2011**
Author: **Matthew Ryan**

CONTACT US

Our Offices

Dublin
33 Sir John Rogerson's Quay,
Dublin 2,
Ireland.
Tel: +353 1 667 0022
Fax.: +353 1 667 0042

Boston
26th Floor,
225 Franklin Street,
Boston, MA 02110,
United States of America.
Tel: +1 617 217 2866
Fax: +1 617 217 2566

New York
245 Park Avenue
39th Floor
New York, NY 10167
United States
Tel: +1 212 792 4166
Fax: +1 212 792 4167

Tokyo
12th Floor,
Yurakucho Itocia Building
2-7-1 Yurakucho, Chiyoda-ku
Tokyo 100-0006, Japan
Tel: +813 6860 4885
Fax: +813 6860 4501

e-mail: enquiries@dilloneustace.ie
website: www.dilloneustace.ie

Contact Points

For more details on how we can help you, to request copies of most recent newsletters, briefings or articles, or simply to be included on our mailing list going forward, please contact any of the team members below.

Paula Kelleher
e-mail: paula.kelleher@dilloneustace.ie
Tel : +353 1 673 1759
Fax: +353 1 667 0042

Breeda Cunningham
e-mail:
breeda.cunningham@dilloneustace.ie
Tel : +353 1 673 1846
Fax: +353 1667 0042

Matthew Ryan
e-mail: matthew.ryan@dilloneustace.ie
Tel : +353 1 667 0022
Fax: + 353 1 667 0042

DILLON EUSTACE

DUBLIN BOSTON NEW YORK TOKYO

33 Sir John Rogerson's Quay, Dublin 2, Ireland.
www.dilloneustace.ie

In alliance with Arendt & Medernach