Legal Issues in Cloud Computing – Part I

by Nick O' Connell - n.oconnell@tamimi.com -

December 2012 – January 2013

Remote access computing services, whereby software applications, databases, data storage, network configuration and programming tools are made available to clients as a service, are becoming increasingly popular. Cloud computing allows businesses to convert capital expenses associated with IT systems and infrastructure into operating expenses associated with platforms, capacity and applications.

For many companies the business case is compelling. As with any business decision, it is important to be fully informed, and aware of the risks. In this article, the first in a series of two, we look at some of the core legal considerations associated with cloud computing.

Information

As one might expect, issues relating to information are central to legal considerations associated with cloud computing. Many of the information-related issues that arise are closely inter-related. By signing-on with a Cloud Service Provider, and moving data to the CSP's cloud, the CSP's client is no longer in direct control of the data. Depending on the nature of the cloud (public, private or 'hybrid'), the potential vulnerability of the data may vary. In some instances, where the CSP uses infrastructure located abroad, data is sent outside the client's country. When data comprises personal data (such as information relating to the client's customers or employees), the client needs to be particularly aware of its obligations with regard to data protection. In the UAE, the processing of personal data may be subject to the Penal Code prohibition on the disclosure of 'secrets' without the consent of the person to whom the secret relates. Other laws may also be applicable where the personal data involves health insurance, medical records, and credit information. For entities in the Dubai international Financial Centre and Dubai Health Care City, specific European-style data protection regulations also impact on the processing of personal information and sensitive personal information, including with regard to whether permission is required to transfer the data to another jurisdiction.

Before signing on with a CSP, the client should familiarize itself with the legal obligations relating to its handling of personal data. When negotiating the terms of service, the client should ensure that the agreement does not permit the CSP to engage in any conduct that would be inconsistent with the client's own obligations in respect of personal data. The client should also consider whether there might be any practical aspects of its privacy obligations that the CSP's system would need to accommodate. (By way of example, in some jurisdictions, compliance with data protection regulations may require the ability to annotate records to reflect objections raised by the data subject. If the CSP's system cannot facilitate this requirement, this may result in the client failing to comply with its legal obligations.)

Security of information is another important consideration. ISO 27001 is a standard that details requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an information security management system. It acts to formalize specific criteria for a range of IT security-related processes, including: information classification and handling; third-party access; incident management and communication; disposal of media; hiring, discipline and termination of staff; acceptable use of computer equipment; development processes; release and change management; and data access, availability and integrity. As part of its due diligence, a client should aim to engage CSPs that can show they are compliant with ISO27001. This

certification illustrates that the CSP has implemented a wide range of security and privacy controls at all levels of its business and that all its employees have been educated in relevant security and privacy issues. The client should seek to build compliance with ISO27001 into the terms of service as a means of ensuring that the CSP will treat information security with the level of attention it requires.

Rules governing document retention are another point to bear in mind when considering a move to the cloud. In the UAE, the Commercial Transactions Law (Federal Law No. 18 of 1993) sets out general requirements for the retention of commercial records, requiring that such records be retained for a minimum period of five years from the date of issue or receipt. With limited exceptions, the Electronic Commerce and Transactions Law (Federal Law No. 1 of 2006) provides that, where it is required by law to retain a certain document, record or information for any reason whatsoever, the retention requirement shall be considered met if the document, record or information is stored in any electronic form. When engaging a CSP to manage commercial records, the client should focus on making sure that the terms relating to the document retention period are consistent with the requirements of the client's own jurisdiction – and not with those of the CSP.

In some instances, CSPs may consolidate the data of multiple clients in order to determine data usage patterns, business trends and strategies. If this type of use is undesirable, then the client should seek to have the terms of service prohibit the CSP from monitoring data usage and from using such 'confidential information' of the client other than for the purpose of providing the cloud service to the client. (Such a restriction would, of course, be additional to any broader confidentiality provisions that should be specified in the agreement with the CSP.)

A further consideration relates to the location of the client's data when it is held in the cloud. In many jurisdictions, the government can require CSPs to disclose client data. In some jurisdictions, the law specifically protects data stored in the cloud from access by the government without due process. In other jurisdictions data stored in the cloud may be disclosed to governmental authorities without due process. Depending on the nature of the data, and the business of the client, it may be advisable to confirm with the CSP the location in which data will be held, and verify independently whether there are any local law concerns in such jurisdiction. It may also be appropriate to agree with the CSP that data will not be held in certain jurisdictions.

Al Tamimi & Company's Technology, Media & Telecommunications team regularly advises on IT service agreements, including in a cloud context, as well as related issues such as data protection, document retention and confidentiality provisions. For further information, please contact David Yatesd.yates@tamimi.com or Nick O'Connell n.oconnell@tamimi.com.