Cloud computing in the UAE: Legal risks and remedies for providers and users

David Yates
d.yates@tamimi.com

June 2011

The term “cloud computing” is often used to describe a broad range of remote access computing services, many of which have been around for a number of years. However, these days a cloud computing environment is generally one in which users have access to applications and data storage services on demand and delivered over an external network, on a user-pays basis. Providers also draw a distinction between public and private clouds, but the focus of this article will be on public cloud services.

The term “legal risks” in this context refers to issues that may expose a cloud provider or user to legal liability, issues which arise from an applicable legal system, and issues which can and should be addressed from a legal perspective in order to create an effective and trustworthy cloud services relationship. The UAE does not have a comprehensive set of laws, regulations and/or official standards specifically for the provision of cloud computing services, and general laws apply. In the absence of a prescriptive legislative framework, however, providers and users must come together in a relationship of trust in order to facilitate the use of a financially advantageous service relationship.

In terms of risk management, users of cloud services are often placing in the hands of third parties responsibility for direct control of critical data and applications. If there is an outage or a security breach, the cloud user could be exposed to claims from its own customers, a failure in business continuity, and potentially reputation damage, even though the cloud provider or a third party telecommunication service provider was responsible for the default. Many SME’s will investigate cloud services and be presented with a service contract which offers the cloud services “as is”, without the cloud provider assuming any risk, and with an exclusion of the cloud provider’s liability to the extent permitted by applicable law. Whether or not a cloud provider and cloud user negotiate a services contact will depend on the parties and the value of the contract. However, even if SME’s must accept stand terms without negotiation they should conduct serious due diligence and contingency planning to mitigate exposure to legal risks.

The claims which a cloud user may bring against a provider when things go wrong, outside the scope of contractual rights, are limited and may not prove to be effective – particularly if the cloud provider is located offshore. For instance, claims for compensation under the UAE Civil Code (number 5 of 1985) will require the cloud user to prove the value of the loss claimed, and this might be difficult. The UAE Federal Law number 2 of 2006 concerning Cyber Crimes focuses on the criminal actions of the hacker, but does not provide a framework which specifically addresses the claims which a cloud user may have against a faulty cloud provider. Other than the law applicable in the DIFC, there is no single data protection / privacy law in the UAE, and the range of laws which speak about the protection of secrets (for instance the Penal Code) do not provide a detailed legislative framework that might protect cloud users from the mishandling of personal and sensitive information. The UAE does not have an information security law as such. However, there can be information security policies which are of vital importance to individual organizations and government departments. For instance, the Abu Dhabi System and Information Centre has developed and implemented an information security policy under Federal Law number 1 of 2006 concerning Electronic Transactions and Commerce with which Abu Dhabi government entities must comply. Ironically, this places added pressure on Abu Dhabi government entities who wish to outsource applications and data storage to a cloud provider, as it is the government entities who nonetheless remain

subject to the obligation to be compliant with the ADSIC information security policy.

In the space available it is not possible consider all of the legal / contractual issues arising, and the following points are a summary of some key issues:

- Data location – Users must consider the impact of the various UAE laws governing the privacy of secrets on the collection and transfer of data to the cloud provider, and the movement of that data across different jurisdictions as part of the provision of the cloud service. Further, what will be the impact, upon the delivery of the cloud services, of the various laws governing data transfer and use which are applicable in the different jurisdictions across which the data is moved?
- Record retention obligations – Under Federal Law number 18 of 1993 Commercial Transactions Law, organizations in the UAE have clear record retention obligations. Under that law, and under the Electronic Commerce and Transactions law, many such records may be kept in electronic form. However, if data storage obligations are outsourced to a cloud provider, the UAE company must ensure that there are adequate protection mechanisms such that a failure by the cloud provider does not result in the UAE company failing to comply with its local record retention obligations.
- Data ownership – Under the cloud arrangement, the cloud user will generate data in the ordinary course of business which is stored in the cloud. However, the cloud provider also will be creating data in relation to the cloud user. The cloud user's ownership rights over all data which it creates and which is created on its behalf by the cloud provider must be firmly established in the service contract.
- The providers in the cloud relationship – Cloud services can be provided by multiple parties working together, and sometimes the user may not appreciate the different parties involved. It is important for the cloud user to know whether it has a directly enforceable contract with the key players in the relationship or whether it is relying on those with whom it does have a contract to enforce relevant terms against other providers.
- Data security – The cloud user will have its own data security and access management policy internally. The cloud user must determine how to ensure that its security measures are reflected in the data hosting service offered by the cloud provider.
- Availability – Cloud computing services inevitably will experience outages and performance slowdowns. While a provider may agree in a contract to give 99.95% reliability excluding scheduled maintenance downtime, the cloud user must nonetheless have sensible options if, for whatever reason, the cloud provider cannot meet that target.
- Planning for the end of the cloud services relationship – Cloud users must avoid a situation, to the extent possible, where the applications and data storage mechanisms which they are provided by a cloud provider do not lock the user into the provider's services, in that a transition to another provider may not be possible without expending significant cost and time in restructuring.
  Cloud users should conduct thorough due diligence of the provider they are considering and in particular focus on the privacy and security levels of the services to be offered. It is in the interests of cloud providers to make this information available and for the parties to act reasonably in contractual negotiations in order to bring about a relationship of trust.