Cloud Computing – Key Issues to Consider in Service Agreements

Datacentre Dynamics have forecast that the Middle East will increase investment in data centre facilities by 46% in 2012 to approximately US$2.12 billion. The industry body also conducted an additional survey of data centre executives around the world in 2011 – the results of which predicted that the Middle East's total spending on IT infrastructure will increase by 18.6% next year to $630 million. New data centres in the region are expected to increase by 6% to 6,400 in 2012. One of the largest drivers for this increase is the growth of 'cloud computing'. This article focuses on some of the key legal or contractual issues in cloud-based infrastructure service agreements.

There is still seemingly a large misunderstanding of what the 'cloud' is. In its simplest terms, the 'cloud' means hardware that isn't physically located on your premises or managed by you, but which is accessed by computers that you use. Imagine the servers you keep in some room down the hall, are actually in a datacentre somewhere else, still connected to the computers in your office, only now you are connecting to them over the internet rather than by direct cross-connects in your office; and, maybe, you no longer purchase a license for the software on those servers, but instead you pay an annual subscription fee per user. Now you are in the cloud. The trick with cloud computing, just like anything else, is knowing what you should be looking for. This is true from a technology perspective as well as from a legal and contracting perspective.

An initial question many organisations raise is 'where will my data be?' The cloud is hardware connected to other hardware, so the answer is that the data is located wherever the cloud provider's servers are located. For some regulated industries or businesses that handle sensitive personal information like banks or healthcare providers, this is not an academic question, as they need to be aware of what regulatory regime their data is subject to. Therefore, if the physical location of your data is important to you, you simply need to ensure that your cloud provider gives you the contractual commitment you need that it will be at all times be kept within whatever country or countries you specify.

In terms of privacy compliance, larger organisations are often tempted to impose their own policies on the service provider, such that the service provider agrees to be bound by the customer's privacy policy (or other policies). Bear in mind that virtually all of these service providers have standards, policies and practices that they apply uniformly across their facilities, and are often entirely incapable of modifying these on a customer-by-customer basis. As a customer, it will be your responsibility to ask the right questions about the service provider's practices and make your own determination about whether your use of their services is a breach of your own policies.

Consider the quality of the service. Your cloud-based services will probably be so-called 'mission critical' services for your organisation, so you will want to take comfort from the fact that the provider is going to be up and running virtually all the time. After all, less (or no) downtime is theoretically one of the benefits of outsourcing IT infrastructure. Look for a strong service level agreement (SLA), which promises both power and bandwidth uptime of at least 99.999 percent and has meaningful remedies if that threshold is not met (usually all or part of the monthly fees for that service). SLAs are notoriously riddled with exclusions and limitations.

Building appropriate protections, standards and service levels into your contract is all very well, but you must also ensure you have the right to audit the service provider's performance. Service providers will quite legitimately resist overly intrusive audit rights, and will likely ensure that any such rights are subject to close supervision. Your right to audit the provider's compliance with its contractual obligations must be balanced against the provider's need to keep its facilities protected from third parties, for both security and business reasons. Remember, these will be shared facilities, and if they give you that right, they give everyone that right.

Limits of liability are key, and are almost always a focal point of negotiations. The contractual commitments of data protection, privacy, quality, reliability and standards become much less meaningful if the provider is not liable for anything more than, say, six months of service fees. How much help will that be when you are facing a disastrous and public privacy breach? At the same time, a provider cannot possibly accept unlimited liability for whatever loss your business suffers due to data loss or business interruption because of downtime. It is common to have a general limit of liability (something high enough to be a serious disincentive to the provider), with much higher limits for things like privacy or security breaches or for the provider's gross negligence. Don't think of your service provider as an insurance company but do hold them to account for what they control.

While these are only a few of the key issues to bear in mind when negotiating a service contract for cloud-based infrastructure services, I hope the theme is becoming clear: cloud computing has its risks, but there are appropriate ways to manage those risks that are fair to both parties. The technology is sound – all you need is a sound contract.

AFRIDI & ANGELL
LEGAL CONSULTANTS

Afridi & Angell
P.O. Box 3961
Al Ghaith Tower - Level 8, Suite 806,
Hamdan Street, Abu Dhabi, U.A.E.
Tel: (971-2) 627-5134
Fax: (971-2) 627-2905
abudhabi@afridi-angell.com

P.O. Box 9371
Emirates Towers - Level 35, Sheikh Zayed Road, Dubai, U.A.E.
Tel: (971-4) 330-3900
Fax: (971-4) 330-3800
dubai@afridi-angell.com

P.O. Box 5925
Al Safa Building - 2nd Floor, Al Boorj Avenue, Sharjah, U.A.E.
Tel: (971-6) 568-1062
Fax: (971-6) 568-2336
sharjah@afridi-angell.com