DLA PIPER

MAY 2014

TECHNOLOGY UPDATE

SELLING CLOUD COMPUTING TO GOVERNMENT: BEYOND THE PRIVACY AND SECURITY DEBATE

ALIGNING GOVERNMENT NEEDS WITH CONTRACTUAL STRATEGIES

By Caroline Atkins and Katherine Armytage

Cloud computing is a major trend in today's ICT environment. However, unlike participants in some other sectors, Governments in the Asia-Pacific region have been slower to take up the significant financial benefits that this technology stands to offer. One major reason for this is the concern about privacy and security, which has received much attention from commentators to date.

However, as the technical issues needed to ensure adequate privacy and security of cloud solutions are gradually addressed and resolved, and Governments become more convinced that cloud computing is a viable option for at least some of their ICT needs, it is becoming apparent that there are other contractual issues acting as barriers to the successful uptake of cloud computing by Governments.

Cloud service providers wanting to make further in-roads into Government cloud computing markets need to understand what these other issues are when designing the contractual arrangements for their cloud computing offerings. Although cloud computing is sometimes described as "old wine in new bottles" (that is, the legal issues are similar to or the same as in traditional ICT contracting, just the packaging is different), there are a number of sector-specific issues that cloud service providers would be wise to consider from a strategic viewpoint when endeavouring to sell cloud computing to Governments.

CONSIDER BUILDING IN A NEGOTIATION STAGE

Many cloud service providers still offer a "take it or leave it" contract for their cloud computing services, particularly public cloud offerings, on the basis that cloud computing is a standard service with standard terms.

These standard contracts typically contain clauses that governments, as publicly funded entities governed by financial and other legislation, cannot accept. They also rarely contain the clauses required as "standard" for doing business with a particular Government. To date, there has been somewhat of a mis-match between the expectations

of Government and cloud service providers as to what should be the "standard" terms.

Some of the more sophisticated cloud service providers are now starting to recognise that the "one-size fits all", heavily pro-vendor, public cloud contracts do not meet the needs of particular sectors, including government. To remain or become cloud computing leaders, cloud service providers should consider implementing a strategic approach that enables their standard contract terms to be considered by and, if necessary, tailored for particular sectors. In particular, cloud service providers need to have efficient internal approval processes for considering any key differences between the terms proposed by a customer in its request for tenders or other form of procurement request (an approach commonly adopted by larger customers and governments) and the cloud service provider's standard contract terms, as well as an effective mechanism to implement any agreed differences (whether through an amended agreement, a side letter or other mechanism).

RECONSIDER USE OF HYPERLINKED AND USER TERMS

Cloud contracts often incorporate by reference other terms, conditions and information located on publicly available web pages (Hyperlinked Terms) and/or specify that other terms and conditions (User Terms) will be incorporated by a user upon entry to the cloud (eg through the use of an "I accept" or "I agree" checkbox which pops up before entry is permitted), both of which may be changed unilaterally by the cloud service provider.

Use of Hyperlinked Terms and User Terms raises some serious problems for Government customers, particularly where they are governed by legislation with criminal sanctions or other consequences for regulatory breaches (eg failure to follow the appropriate approval mechanisms for financial expenditure or changes to common law liability arrangements). Whilst individual users can accept User Terms (which they may do without considering the implications), or when the terms of the contractual arrangements can be unilaterally changed, there is a real risk of regulatory breach.

Governments need contracts for cloud computing services that are clear and complete, with approved change control mechanisms, to ensure they comply with all laws and policies surrounding their entry into contractual arrangements. This can be achieved through a range of strategies, including:

- excluding Hyperlinked Terms or User Terms;
- including a "general override" clause expressly excluding Hyperlinked Terms and User Terms that are inconsistent with the master contract;
- including a "specific override" clause so that the master contract terms override other terms to the extent they, for example, increase costs or change liability or licence rights; or
- "locking in" all Hyperlinked Terms and User Terms as at a particular date with agreed change control measures.

PROVIDE APPROPRIATE USAGE AND ACCESS RIGHTS

Cloud service providers often argue that, because a contract is for the provision of a service, it is not appropriate to include licence or usage rights in the contract at all. Alternatively, some cloud service providers only include minimal, or poorly defined, access and usage rights to their cloud services in their contracts. Governments are unlikely to be convinced by this as, like most customers, they need to be certain about the service they are purchasing and ensure that their required usage and access rights are clearly set out in the contract without undue restrictions.

Governments also need to ensure that the contract permits access by all types of required users, including contractors and members of the public who receive their products and/or services. Access will also be required to enable the transfer of data held in the cloud back to the customer or another entity upon expiry or termination of the contract.

CONFIGURATION AND INTEGRATION OF CLOUD SERVICES

Many cloud services require integration to effectively meet a customer's requirements. Often a contract with an entity which is not the cloud service provider is entered into for these services. Having two contracts for one solution immediately gives rise to the risk of debate about the division of responsibility and the extent to which each supplier is responsible for the solution.

It is important that each contract accurately reflects the promises made by each supplier about the

extent to which the product and/or services will meet the customer's specific requirements. In addition, it is important to ensure the division of responsibility between the suppliers is clear and that they are obliged to work together to solve any problems.

Contract mechanisms used in systems integration contracts are of value in dealing with cloud service integration requirements.

ALIGN PERFORMANCE STANDARDS AND REMEDIES TO THE CLOUD SOLUTION

Standard cloud computing contracts often contain no, or very limited, performance or service level standards. They also often have liability provisions which are very favourable to the cloud service provider, with very broad exclusions of and low limits on liability (often less than the total amount that the customer has paid for the services provided).

It is clear from the various forms of cloud computing contracts that many cloud service providers do not recognise that Governments, as publicly funded entities, usually have very strict rules and regulations around managing their liability.

In addition, at the most basic level, Governments want a cloud solution that works. Government customers are likely to view favourably contracts which have sensible performance levels specified, or at least a workable incident or outage management regime to ensure that, if a problem arises, the cloud service provider is obliged to fix it promptly. There should also be consequences if the required level of performance is not achieved. These may not always be directly financial (eg service credits), as Governments also value non-financial consequences (eg provision of additional services at no cost or the requirement to comply with a back-up plan/alternative option if the cloud service is unavailable for an extended period of time).

Carefully consider privacy and intellectual property issues

Much of the focus to date has been on whether the technical aspects of a cloud solution are capable of ensuring that, when data is placed in the cloud, the strict privacy and security requirements needed to protect Government data (which often includes personal, sensitive or otherwise confidential information) are met, and on ensuring that the contract imposes the necessary obligations on the cloud service provider to ensure that the Government meets its obligations.

However, beyond this, standard cloud computing contracts are also rarely tailored to adequately deal with intellectual property issues involving:

- Government material that will be uploaded into the cloud and stored on the cloud service provider's infrastructure (including data, data schemas, business logic and/or programs);
- material generated using the cloud (eg databases or reports); or
- changes to pre-existing software and infrastructure for a particular Government client (particularly relevant for private and community cloud offerings).

Governments are required to protect certain types of data held by them through a range of domestic legislation and international obligations. Often, standard cloud computing contracts grant cloud service providers extensive and perpetual rights to use and reproduce material uploaded to the cloud, or generated using the cloud, without notice or consent. They also sometimes allow the disclosure of confidential information or the re-deployment of material to other clients without approval. For many Governments, accepting such clauses would lead to them being in breach of their legal, privacy and security obligations.

Cloud service providers which are prepared to work with government customers to ensure they do not have use or disclosure rights that are not strictly necessary to provide the services, and which could lead to a breach of the customer's privacy and security obligations, are likely to have a strategic advantage in the government market.

After expiry or termination of the contract

Cloud computing contracts are also typically silent on what happens when the contract ends. Governments are, in the ordinary course of things, an enduring and perpetual entity, and they need to ensure a smooth, seamless transition of their operations when a service arrangement comes to an end. In particular, Governments need to see cloud computing contracts which ensure:

- their data and materials will not only be returned at the end of the contract, but will be returned in a format that enables them to interpret the data; and
- all data and materials will be returned or destroyed, including low level data (such as cyclical backups and data mirrors) which may remain in the cloud after transition of substantial data, with independent verification.

Conclusion

Cloud computing is a new and exciting, but still emerging, area for Government ICT contracting in the Asia-Pacific region. It represents an as-yet largely untapped market for cloud service providers, of significant size and importance.

However, cloud service providers need to remember that Governments are not directly equivalent to large corporate enterprises. They are governed by different legislative arrangements and have different drivers, goals and requirements. Attempting to win a share of this market without understanding these differences is unlikely to be successful.

In this article we have outlined some of the general concerns often experienced by Government customers when reviewing a cloud computing contract. There will always be other issues, depending on the jurisdiction in which the Government is based. However, cloud service providers which take a strategic decision to consider the issues identified in this article, and develop product offerings tailored to meet the particular needs of Governments in their jurisdiction, will be well placed to achieve a substantive and workable contract, which will be key to achieving a successful cloud computing outcome.

www.dlapiper.com

MORE INFORMATION

For more information, please contact:

Caroline Atkins
Partner
T +61 2 6201 8789
caroline.atkins@dlapiper.com

Katherine Armytage
Special Counsel
T +61 2 6201 8766
katherine.armytage@dlapiper.com

Contact your nearest DLA Piper office:

BRISBANE

Level 28, Waterfront Place
1 Eagle Street
Brisbane QLD 4000
T +61 7 3246 4000
F +61 7 3229 4077
brisbane@dlapiper.com

CANBERRA

Level 3, 55 Wentworth Avenue
Kingston ACT 2604
T +61 2 6201 8787
F +61 2 6230 7848
canberra@dlapiper.com

MELBOURNE

Level 21, 140 William Street
Melbourne VIC 3000
T +61 3 9274 5000
F +61 3 9274 5111
melbourne@dlapiper.com

PERTH

Level 31, Central Park
152–158 St Georges Terrace
Perth WA 6000
T +61 8 6467 6000
F +61 8 6467 6001
perth@dlapiper.com

SYDNEY

Level 38, 201 Elizabeth Street
Sydney NSW 2000
T +61 2 9286 8000
F +61 2 9286 4144
sydney@dlapiper.com