Dechert LLP

Gearing Up for the Complicated Worlds of Outsourcing and Offshoring

May 14, 2012

In this issue

This update was authored by Vivian A. Maese. If you have questions or for more information, please contact:

Vivian A. Maese
New York
+1 212 698 3520
Send email

Timothy C. Blank
Boston
+1 617 728 7154
Send email

Kate Tebbutt
London
+44 20 7184 7518
Send email

Joshua H. Rawson
New York
+1 212 698 3862
Send email

Renzo Marchini
London
+44 20 7184 7563
Send email

Henry Wang
Beijing
+8610 5829 1318
Send email

To see the full list of outsourcing lawyers, please visit our website.

Dechert LLP

Gearing Up for the Complicated Worlds of Outsourcing and Offshoring

Head in the Cloud? Achieving Savings While Managing Risks in the United States

What is “the Cloud”? That depends on whom you ask. Answers currently run from Apple and its competitors offering storage and music and file synchronization to customers who are individuals, to very large vendors at a global scale servicing very large enterprises as customers. This is a frontier in many ways, and if you are going to embark on a Cloud transaction, you will be well advised to ask many questions, some of which may seem basic. While this article is focused on the laws in the United States, the risk management suggestions highlighted here are applicable anywhere on earth.

Fundamentally, moving to the Cloud is an outsourcing transaction, i.e., a company engages a third party to perform a function that the company would otherwise have performed for itself. Cloud computing is a business model that enables organizations to achieve potentially significant cost savings by sharing services, software and platforms in a third party’s data center, instead of operating in the company’s own data center.

Often Cloud providers will dazzle the prospective client with the potential for very significant cost savings, which is very alluring in this economic climate. The mode of operation used by some important name brands in the Cloud space is to put a “standard form contract” in a prospective client’s hand accompanied by a smile and a request that you “sign here.” Don’t do it! Don’t sign a standard form for something as important as a data center, which is the heartbeat of your operation. Go directly to your lawyer. This warning is especially relevant to regulated financial services institutions. If you sign the standard form and you are subject to any type of risk management governance-related obligations, which is the duty of every Board of Directors, you may not be able to demonstrate that the company has adequately managed its risks. Risk management functions for financial institutions after Dodd-Frank are especially highlighted. For example, FINRA has a list of examination priorities for 2012, and cybersecurity and outsourcing are on that list. It is unlikely that the vendor’s standard form, drafted for its purposes, will provide the company with the control and assurances that it will need when FINRA examiners arrive.

Not intending to alarm, but if a data center is being replaced by a Cloud provider, it is a “bet the farm” transaction.

Remember: great deals begin with great due diligence. Conduct your due diligence assiduously, and negotiate carefully, especially if you are in the financial services industry.

What follows is focused on financial services companies, but many issues of control over data and processes and the ability to have continuity of business functions are applicable to any company considering Cloud services.

In financial services, you must take account of the important macro-regulatory compliance themes for U.S. financial services companies, which include:

- Dodd-Frank Act and related Bank & Securities Financial Stability Outsourcing Regulations;
- Sarbanes-Oxley Section 404;
- Laws pertaining to Cybersecurity and Data Privacy; and
- Record Retention.

Here are a few starting points.

1. Performance First

Can the Cloud provider actually do the job that you need done? Getting an answer will require a great deal of conversation with the prospective vendor. Consequently, all discussions with a Cloud provider should begin with a Non-Disclosure Agreement. Your company will want to protect its proprietary information during the conversation. In order to determine whether the Cloud provider can actually provide what you need to run your business, you will necessarily be sharing a lot of information. During the early days of the conversation, your company will need to disclose to the Cloud provider a fair amount of information about procedures and processes and data that may be competitively sensitive.

Also during the initial stages, probe how quickly the Cloud provider recovers services and data if there is a failure of the technology for any reason. Almost perfect uptime for on-line capabilities, and very well devised and operated data protection are fundamentals in your own data centers, and they must be present in the company's Cloud arrangement. A relationship with your Cloud provider relies on trust – once they are hired, they are not easily fired. Verify capabilities in advance, and write a contract that allows you to continue to monitor and react if things change during the contract's term. The company should be comfortable with the Cloud provider they select and this aspect of due diligence will go a long way to ensure that comfort.

Importantly, you should ensure that the Cloud provider understands what it is getting into. Depending on the substance of the service being provided – for example, support of a consumer banking application – the Cloud provider needs to understand that bank regulators may examine the Cloud provider as if it is a regulated entity.

The post Dodd-Frank outsourcing regulations – effective and proposed – are clear that when a company outsources a function, the company is not off the hook for regulatory compliance. Do a careful inventory of the regulations that pertain to the service(s) that you propose to move to the Cloud, validate that the Cloud provider can perform the functions and clearly document your needs in the Cloud agreement. Be sure that you have contractual and actual capabilities to audit and require corrective actions and even terminate if necessary so that your company's obligations to regulators can be satisfied, and the Company's own internal operational risk management requirements are met.

Cloud providers that understand the culture of regulatory compliance will likely be a better fit for a financial services company. Having a Cloud provider that is learning on the job isn't a good idea.

2. Cybersecurity and Data Privacy

Two areas of very intense focus by financial services regulators at present are cybersecurity and data privacy. When thinking about these issues in the Cloud, the Company really does need to create an inventory at the data element level to understand the kind, character, and privacy/cybersecurity implications of the information the Company will entrust to the Cloud provider. Is it information that relates to a person that may be sensitive like social security numbers, financial account identifiers and balances, or employee health information? Identifying the location of the servicer of the data (your Cloud provider may have locations in multiple jurisdictions), where will it be housed, where in the world it might be sent or reside? Do the involved jurisdictions have laws and regulations that impact your business, or your obligations to manage the data? For example, is personal information coming from a country that has data protection legislation/regulations that requires notification of the individual as to how that information is being used? Do you or does the Cloud provider have the necessary capability to make such notifications? Which of you will absorb the costs in the event the data is lost or stolen, if any? Is the information entrusted to the Cloud proprietary or otherwise valuable intellectual property such as trading algorithms or a database of corporate client information? If so, evaluate the information according to its criticality to your business – will the loss or corruption or misappropriation of the information create an operational or legal problem, or perhaps do reputational harm or cause you direct economic loss or enable a competition?

After the company understands its own position, it can begin to evaluate the security of the Cloud provider. Often a map or diagram of the flow of information from the company to the Cloud provider and back, or to and from other destinations, and can help you to understand how and where the data moves, and what procedures, processes and technologies are in place to keep the data safe and protected at each step.

Bad actors in cyberspace are increasing both in number and sophistication. The Company should ascertain that your Cloud provider has a dedicated, highly competent Cybersecurity staff that has high visibility and respect in its own organization. During conversations find out whether the Company focuses on dealing with the continuous evolution of "hacker" incursions into on-line operations. Some

additional things to look for in a Cloud provider are background checks for employees, qualification and standards for those employees, and a culture sensitive to security issues. Important basic questions include: Is the company's data encrypted during transmission? While it is in storage? Is their employees' access to data restricted to people assigned to your account? Do those people also work on your competitors' accounts? Are there sub-Cloud providers? If so, have the Cloud – sub-Cloud relationships and interactions been subject to the same scrutiny as you are applying to your contract with the Cloud provider? What is the Cloud provider's process for removing data ("scrubbing" the disks and the memory) when equipment is replaced or upgraded? What happens to your company's data when the contract expires? Are transition services back to the company or to another Cloud provider carefully considered and documented? What provisions are in place in the event that the contract with the Cloud provider is terminated?

If your company is a public company, the Securities and Exchange Commission, Division of Corporate Finance, CF Disclosure Guidance: Topic 2 – Cybersecurity, October 13, 2011, requires your company to disclose risks specifically associated with outsourcing transactions. Will your contract with a Cloud provider support you in documenting the existence of risks (and the approaches in place to mitigate them)?

Cloud services agreements, like any other outsourcing arrangement, need to fit into the company's overarching rubric for risk management. The company needs to assure itself, and to be able to assure its Board, its shareholders and its clients if called upon to do so, that the Cloud provider is secure, safe, and well managed, before contract execution. Furthermore, the company needs to be in a position contractually to ensure that the Cloud provider stays that way for the life of the contract. Think through what your contingency plan will be if there is a degradation in the service provided during the contract term, or there is a problem in the region where the services are provided.

3. Disaster Recovery Capability

Here again, you should think about what you would expect from your own data center operators, and this will give you a base line to this important consideration when managing operational risks. Be sure you have reviewed and are satisfied with the Cloud provider's approach to disaster recovery.

4. Record Retention (and Retrieval)

Once you have begun to operate in the Cloud, your company is no longer in direct command of its data. Record Retention and the ability to preserve and retrieve records comprehensively and quickly for company business, investigations, examinations and litigation is important. Make sure that the company's contract with the Cloud provider is consistent with the regulations and the required procedures in the event of a litigation (e.g., can the Cloud provider perform the steps necessary for a litigation hold on the records or email in their custody?) Jurisdiction in the Cloud is not necessarily intuitive. A useful step is to designate a jurisdiction in your contracts.

Be careful that arrangements for Record Retention, which often involve third parties, are modified to give you control of your data during and after the contract.

5. Other Issues

While we have addressed many questions here. The list is comprehensive, but not exhaustive. Your business will have its own related considerations. Another area that will be of concern to most companies pertains to tax issues depending on the location(s) of the service provider and the company, and related factors implicating permanent establishment or transfer pricing.

* * *

Moving to the Cloud, which sounds easy, is anything but easy from a legal point of view. Nevertheless, the level of care suggested here is needed. At the end of the day, the Company will want to actually realize its anticipated savings, and not be unhappily surprised months or years into the relationship.

Return to Table of Contents.

Dechert LLP

Gearing Up for the Complicated Worlds of Outsourcing and Offshoring

Country Risk: Illustrated

Last time, we wrote about “country risk”; i.e., the risk a company takes by doing business in a different country, where laws might be different from what you might expect in your home country.

Since then, a case has been decided in Mumbai, India before the Controller of Patents that illustrates the need to take country risk into account when selecting offshore locations.

In the matter of Natco Pharma Limited (Natco) and Bayer Corporation (Bayer), Natco applied for and was granted a compulsory license under Section 84(i) of the Patents Act, 1970. Under the patent law in India, a compulsory license is an involuntary contract between a willing buyer and an unwilling seller imposed and enforced by the State – essentially the government permits someone else to produce the patented product without the consent of the patent holder.

In this case, Bayer, an American company headquartered in Pittsburgh, PA, invented a drug useful in the treatment of cancer. Bayer was importing and selling the drug in India, and presumably expected protection of their patent rights to be the exclusive supplier of the drug. The compulsory license applicant was Natco Pharma Limited, an Indian company headquartered in Hyderabad, and a manufacturer of generic drugs. Natco approached Bayer with a request for a voluntary license to manufacture and sell the drug; however, the parties did not come to terms, so Natco applied for the compulsory license.

In India, the applicant for a compulsory license must prove that “reasonable requirements of the public with respect to the patented invention have not been satisfied.” Natco argued that Bayer did not take adequate steps to manufacture the product in India; that the drug was priced too high; and, that the drug was only available in hospitals in major cities. Bayer countered, first, that price and access should not be linked; and, further, that because administration of the drug required supervision by specifically trained doctors, the fact that it is not available in villages (where such doctors are not normally available) is not probative.

Bayer presented robust analyses having to do with price, number of patients, number of drug treatments, and distribution; all in support of its position that the drug was appropriately available. In response to the suggestion that the drug was priced too high, Bayer offered to supply the drug to needy patients based upon an oncologist’s recommendation. The Controller of Patents was not convinced. Bayer was required to provide its intellectual property to Natco in exchange for 6% of the net sales of the drug by the Licensee for the balance of the term on the patent. Bayer’s patent rights to be an exclusive supplier were effectively invalidated.

Bayer’s business judgment, and its argument against the compulsory license, that it did not, as yet, need to invest in in-country manufacture of the drug because it could properly supply the Indian market from factories outside India were overridden. In deciding, the Controller of Patents was substantially influenced by the fact that, since the patent had issued, Bayer efforts to commercially exploit the patent in other countries had included in-country manufacturing; but since 2008, when the patent issued in India, Bayer did not have manufacturing facilities for the drugs in India.

Return to Table of Contents.

Gearing Up for the Complicated Worlds of Outsourcing and Offshoring

Consumer Financial Protection Bureau Issues Outsourcing Guidance

On April 13, 2012, the newly minted Consumer Financial Protection Bureau (CFPB) issues CFPB Bulletin 2012-03 on the topic of Service Providers that, while using different words does not vary substantially from the supplier guidance issued on this topic from other financial service regulators, thankfully.

While relationships with service providers are viewed as potentially useful, the bank remains responsible for complying with Federal Consumer law to avoid consumer harm.

In addition to regular bank examinations, the CFPB will have supervisory and enforcement authority over the Service Providers.

An effective process for risk management and governance is expected.

To ensure that the contracts with Service Providers do not pose unwarranted risks to consumers, the following steps are recommended:

- Conduct thorough due diligence to verify that the Service Provider understands and is capable of complying with Federal Consumer financial law;
- Requesting and reviewing the service provider's policies, procedures, internal controls, and training materials to ensure that the service provider conducts appropriate training and oversight of employees or agents that have consumer contact or compliance responsibilities;
- Including in the contract with the service provider clear expectations about compliance, as well as appropriate and enforceable consequences for violating any compliance-related responsibilities, including engaging in unfair, deceptive, or abusive acts or practices;
- Establishing internal controls and on-going monitoring to determine whether the service provider is complying with Federal consumer financial law; and
- Taking prompt action to address fully any problems identified through the monitoring process, including terminating the relationship where appropriate.

Return to Table of Contents.