CARLTON FIELDS

Cloud Servicing Contracts: Legal Considerations for Companies Migrating to the Cloud

March 25, 2013

Demand is increasing for cloud services by U.S. companies in order to reduce costs and increase efficiencies. Those same companies are asking law firms and legal departments to review cloud service contracts submitted by service providers. A migration to the cloud, or a switch between service providers, should only occur after close review of both the technology involved and the terms of the service contract. Generally, at a minimum, companies should examine and consider the following concerns before entering into any cloud services contract.

1. Know Your Regulatory Requirements

Companies should be mindful of industry-specific rules and regulations that govern their respective industries. For example, health care companies must comply with HIPAA and financial services companies must comply with FINRA. In addition to federal rules, virtually all states have laws governing data systems, breach notifications, and data migration.

2. Length of Term, Modification Companies should carefully consider the length of the term of all cloud services contracts. Technologies evolve very rapidly and being locked into a lengthy contract may put your company at a competitive disadvantage by making it unable to keep up with emerging technologies and client demands. Periodic benchmarking and allowing for modifications should be included in cloud services contracts with all providers.

3. Security and Privacy

Few things will damage a company or its brand quicker than a data breach that compromises customer data. In addition to reputational damage, financial losses due to a data breach can be crippling. Companies should thoroughly understand how cloud service providers will use data, and

should further ensure that all such providers have rigorous data security practices and procedures. Typically, the cloud service provider should indemnify the customer for losses suffered as a result of a data breach caused by the vendor's negligence, mistake, or carelessness. Further, the cloud services provider should be required to notify the customer about any hacking attempts regardless of whether any such attempt is successful.

4. Compliance

Generally, cloud service providers should be contractually obligated to comply with all requirements imposed on their client by regulators, industry best practices, and courts. Vendors should also typically indemnify customers for any failure to comply with all obligations imposed on their clients.

5. Termination

Finally, cloud services contracts should include a comprehensive termination clause. Most important, the clause should clearly state that, regardless for the reasons of termination (including customer breach), the cloud services provider must promptly return all of the client's data in a pre-arranged format. A cloud services provider should never be allowed to withhold its customer's data for any reason. Additionally, cloud service providers should be required to provide transition services to migrate data to a new vendor upon termination.

These are just a few of the issues companies should consider when entering into cloud services contracts. Companies should weigh these and other factors such as cost, complexity, and business needs before securing the services of a cloud services provider. All companies should work with experienced technology consultants and legal counsel to ensure that the products and services, as well as the terms of their use, are properly vetted.

Related Practices

Business Transactions
Cybersecurity and Privacy
Intellectual Property

accuracy or completeness of this outside information, nor is the inclusion of a link to be intended as an endorsement of those outside sites.