1115 BROADWAY 12TH FLOOR, NEW YORK, NY 10010
212-710-2643 | linfo@WRLAWFIRM.com | www.WRLAWFIRM.com

Top Questions to Ask Before your Business Stores Company Data In The #Cloud

If you own a business, your IT staff is likely one of many across the globe who are slowly convincing businesses owners and managers that storing data in "the cloud" is the future. He or she probably pointed out that hiring a third party to store your company's data will allow you and your employees to access it from anywhere via the Internet, cut costs, and may help you avoid a great deal of hassle should something happen to the company's on-site data storage facilities. But before you give the green light to your resident tech geek to start outsourcing your company's data storage to the cloud, there are several legal considerations that you should be aware of prior to making the big move. Here are the five major questions that you as a business owner or manager need to know the answers to BEFORE signing a contract with a cloud service provider:

1. Who will have access to your business' data?

The first piece of information that you need to obtain from potential cloud service providers is whether a third party will be processing, storing, or transmitting your company's data. In some cases, a cloud service provider may not actually own the servers where your data will be stored. The cloud service provider may subcontract out the storage of data, and that subcontractor may in turn be subcontracting out storage services, and so on. Other cloud service providers may offer bundles of cloud software services that seem to all be part of one application to the user, but are actually made up of several subcontractors that operate the different services and the associated data storage. The more subcontractors that are involved, the more legal risk your company will likely be subject to because it can never know where the data is physically located and how well it is protected at any one time.

Any contract your business signs with a cloud service provider should address who will actually be handling your company's data, whether any subcontractors will be allowed to further subcontract out the storage of your company's data, whether you will receive notice when your cloud service provider switches subcontractors, and what data security standards any subcontractors should be able to satisfy. It is also important to spell out that although your company is providing the cloud service provider with its data, that does not automatically mean that they own it or are allowed to exploit it or use it for any purpose other than to provide services to your company. The contract should make clear that any intellectual property contained in the stored data belongs to your company, and whether the cloud service provider may allow third parties to access or use your company's data should be addressed.

2. Where will your business' data be stored?

Where the servers containing your company's data are physically located is very important when it comes to complying with various laws protecting the privacy of your customers and regulating how security breaches must be handled. The jurisdiction where the servers with your company's data are kept controls how that data may be stored and accessed. In the US, most states have their own data protection and breach laws for personal or sensitive information. It is your company's responsibility to make sure that these laws are complied with – not the cloud storage service provider's.

Where your data is stored also affects whether the government in that jurisdiction can access that information and how. A potential problem with storing information in the United States is the USA PATRIOT Act, which allows the US government to seize information stored in the US or accessible from the US without giving the affected parties notice, reason, or an opportunity to contest the intrusion. This ability may conflict with privacy laws governing the private data of your customers who live outside of the US.

It is also important to ask whether your company's data can be transferred elsewhere, to where, and whether your company will be notified beforehand. Businesses that have customers located in the European Union need to be aware of the EU Data Protection Directive, which prohibits transferring the personal information of EU residents out of the EU to many countries, including the US, without complying with the applicable provisions of the Directive. Switzerland and Russia have similar data protection laws based on the Directive, and the Canadian province of Alberta's Personal Information Protection Act requires that notice be given to a resident whose personal information is transferred outside of Canada. Your company's data might also be subject to US export control regulations, such as the Export Administration Regulations (EAR) or the International Traffic in Arms Regulations (ITAR), if it is "exported" to a server outside of the US.

If your company is planning on storing the sensitive or personal information of its customers or employees in the cloud, the contract should require the cloud storage provider to comply with all data storage laws in the country or state where the servers with your company's data are located. It is also imperative that you are informed of where your data is or will be at all times to make sure that your company does not violate any international privacy laws or can quickly comply with the data security breach laws of that country or state should the need arise.

3. What data privacy and security measures does your cloud service provider have in place?

Your business needs to not only make sure that its cloud service provider complies with the data privacy and security laws in the physical location where its data is stored, but also the laws that govern the type of data that will be stored there. Unlike the EU, the US does not have a comprehensive data privacy law. Instead, there are several federal laws that apply to the storage and use of only certain types of information. Financial institutions that collect non-public personal information from their customers need to follow the provisions of the Gramm-Leach-Bliley Act. Publicly traded companies storing their financial data in the cloud should ensure that their cloud service provider complies with Section 404 of the Sarbanes–Oxley Act of 2002. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (the HITECH Act) both concern information that can be linked to an individual relating to health status, the provision of health care, or payment for health care. The privacy of student education records is governed by the Family Educational Rights and Privacy Act (FERPA), and the personally identifiable information of children under thirteen that is collected online is covered by the Children's Online Privacy Protection Act (COPPA).

Your cloud storage service provider should be prepared to comply with any of these laws that apply to your company's data, and the contract should specifically provide for such compliance. In addition, your company may want to secure an annual audit right to assess whether your cloud service provider is in compliance with applicable state and federal data security laws.

4. What is your cloud service provider's security breach policy?

Many of the state and federal laws mentioned above set forth steps that must be taken by any company that has experienced a security breach affecting personal or sensitive information. But if your company does not have complete control over the storage of its data, you may not even be aware that the security of that data has been breached. Take careful note of how your cloud service provider defines a security breach and under what circumstances you will be notified. The contract should address what investigative or mitigation measures your cloud service provider must take should a breach occur, as well as whether your company will have the ability to conduct its own investigation into the cause and magnitude of the breach. In the event of a data breach, your cloud service provider's interests may not be aligned with your own (especially if it was the cloud service provider's fault), so it is vital that your company have access to all relevant information surrounding the breach and control over how it is handled.

One of the biggest concerns your company should have when storing data in the cloud is identifying who will be held liable for security breaches. Take special note of any limitations on liability that the cloud service provider claims. The most important provision your company can include in a contract with a cloud service provider is one indemnifying your company for all costs associated with a security breach, including the costs your company will incur related to notification, investigation, litigation, and any fines or penalties it may sustain.

5. How will the move to cloud computing change how litigation is handled?

One issue that may not immediately come to mind when moving your company's data to the cloud is how it will change the process of e-discovery. The statutes and regulations that govern your company's current data policies also apply in the cloud, as well as the obligation prevent the destruction, alteration, or mutilation of potentially relevant evidence when your company reasonably suspects or becomes aware of potential litigation or investigation. For these reasons, you need to be aware of your cloud service provider's data preservation, retention, and destruction policies and must have the ability to place a litigation hold on the destruction of your company's data.

The cloud service contract should also address how both parties will respond to subpoenas or discovery requests and who will bear the costs associated with producing the requested data. If the cloud service provider is served a subpoena or discovery request, issues such as whether your company will be notified, how long the cloud service provider may take to notify you or respond, and whether it will seek a protective order to avoid or limit the disclosure of your company's data should be dealt with in the contract. How your company will access its data and how long the cloud service provider has to provide that access should be specified in the event that your company must comply with a discovery request.
