



Cloud Computing Considerations for Multinationals

Joan Antokol - Partner, Park Legal LLC

Cloud Storage is Unavoidable





Cloud Computing Basics



Definition:



Scalable, on demand resource for computing power and/or computing storage



Fundamental requirements for the provider:

1. Low cost power source (e.g., electricity)

2. Robust telecommunications infrastructure



Competitive Advantage Drivers



Technology



Communication



Scalable



Accessible



Convenient



Cost Avoidance



Data Management Challenges



Where is your company's data?



Is it secure?



Is it available/accessible?



Is it backed up?



Are you in compliance with your legal obligations?



Legal Considerations



Data privacy



Data security



Breach notification



Records retention



e-Discovery, litigation and investigations



Many others



Legal Considerations - Examples



Clinical Research Requirements



Patient Data Requirements



Human Resource Data



Cardholder/Customer Data



Business Data



Recommendations



- Know the geographical location of the data storage, and ensure that the provider will not store/move data to another country without written permission in advance.
- Understand how the cloud provider secures the data and how the provider detects and reports a compromise.
- Know the situations in which a third party or a government can seize the data from the provider. The provider should provide advanced notification of such event.
- Ensure that the cloud provider appropriately protects the data as specified by your agreement, and in accordance with applicable laws such as HIPPA-HITECH, PCI, etc.
- Address access by the provider and the provider's business partners. What types of intrusion detection are in place?
- Be sure that the data is encrypted in transit (and, to the extent warranted, at rest).
- Understand how the provider manages encryption for multiple consumers. Instead of a single encryption key for all consumers, the provider should use (at least) one key per client.
- Be sure that the provider logically isolates the data of your organization in such a way so as to prevent any unauthorized access, loss, misuse, modification, or deletion of the data.
- Verify that the provider destroys deleted data in such a way that it cannot be later recreated.
- Clearly address breach notification requirements and responsibilities in your agreement.



Conclusion

**Remember that your organization is generally held responsible for the misdeeds of your employees...
AND your vendors.**





Thank You!

Joan Antokol

Partner

Park Legal LLC / Park International LLC

10401 N. Meridian St.

Suite 350

Indianapolis, Indiana USA

Joan.Antokol@parkintl.com

+317-616-3350 (Office)

+317-937-6903 (Mobile)

