

**Global Data
Privacy and
Security Team**

Contracting with Cloud Computing Vendors: At A Glance

Most companies now use some form of cloud computing whether through software as a service, platform as a service, or infrastructure as a service. Cloud computing’s cost-effective scalability offers significant advantages to a business, but these advantages simultaneously invite significant security concerns. Even with exceptional diligence, services providers cannot guarantee 100 percent security of the underlying data.¹



To minimize this risk to data security, companies should evaluate the following as they consider cloud computing:

- | | | | |
|---|---|---|---|
| ✓ | Does data need to be stored in a specific jurisdiction? Some jurisdictions require that data remain within their borders. | ✓ | Are the agreement’s terms sufficiently defined to avoid ambiguities over what the vendor has contracted to provide the customer? Trending technology terms often must be defined to ensure all parties perceive them the same way. |
| ✓ | Does the agreement set forth whether the vendor is dedicating hardware to the customer? Absent express language, the vendor is likely providing shared hardware to the customer. | ✓ | Does the agreement guarantee to maintain any current APIs or features, or does it promise to provide future functionality? Depending on the circumstances, schedules can be a useful way to ensure certain necessary functionality remains in the service. |
| ✓ | Does the agreement clearly explain who has rights to the data stored using the service? Depending on the underlying service, some agreements grant the vendor limited rights. | ✓ | Will the network connections between the vendor and the customer provide sufficient bandwidth, and if not, what contractual recourse does the customer have? Although cloud computing is seen as ubiquitous, engineering realities may curb its availability. Customers should consider that risk when contracting. |
| ✓ | To what extent is cryptography used? Is each separate record in the cloud encrypted, or does all data use the same encryption key? The value of these approaches vary based on the nature of the data and the processing costs. | ✓ | Will use of the cloud service conform with the customer’s industry-specific guidelines? |
| ✓ | Who is responsible for backing up data? For example, the Health Insurance Portability and Accountability Act (HIPAA) requires disaster recovery solutions, and customers in that space and others need to ensure that responsibility is fulfilled. | ✓ | Does the agreement give the customer the ability to delete data stored by the vendor and confidence that such deletion can be achieved? For some categories of data, customers must ensure that data is completely removed from the servers. |
| ✓ | Does the agreement set forth standards for how the customer can export its data from the vendor? A customer may want to switch from one cloud vendor to another or may simply want to proceed in a different technological direction. | ✓ | Does the agreement clearly set forth how the parties should communicate in the event of a data breach of service outage? Similarly, does the agreement contain adequate representations about the vendor’s steps to prevent either event? |
| ✓ | Are the appropriate licenses in place to execute software in a cloud computing environment? For example, some software is priced based on the type of server on which it will be run. Meanwhile, the execution of the software in a cloud (or networked) environment may trigger additional considerations. | ✓ | Does the cloud vendor have adequate liability coverage? Although no one wants the agreement to reach that point, the customers should have adequate protection. |
| ✓ | Does the agreement give the customer sufficient flexibility to expand or contract the extent to which it uses the cloud services? One of the advantages of cloud computing is the idea that use can be scaled to match a customer’s needs. | | |

For more information contact:

David A. Zetoony
Partner
david.zetoony@bryancave.com
1155 F Street, N.W.
Washington, D.C. 20004
phone: 202 508 6000

John C. Bush
Associate
john.bush@bryancave.com
One Atlantic Center, 14th Floor
1201 W. Peachtree St., N.W.
Atlanta, GA 30309
phone: 404 572 6798

For additional information,
please visit
www.bryancavedatamatters.com



¹ See <http://blogs.wsj.com/cio/2015/05/01/dropbox-is-not-part-of-security-problem-says-new-security-chief/?KEYWORDS=cloud+computing>

² <http://www.peworld.com/article/2685792/infographic-smb-cloud-adoption-trends-in-2014.html>

³ <http://cloudindustryforum.org/images/PDF/CL0072-Claranet-Research-Report-Adoption-Trends-in-Cloud-Computing-2011-2014.pdf>