April 2014

MAYER·BROWN

ELECTRONIC DISCOVERY & INFORMATION GOVERNANCE

Tip of the Month

Data Privacy Concerns When Moving Email to the Cloud

Scenario:
In an effort to reduce costs and leverage the latest advances in technology, the chief information officer of a multinational company decided to use a cloud computing vendor to host the company's email. After identifying a handful of vendors that appeared to meet the company's needs, the CIO asked each vendor to submit bids and proposed service agreements. Aware of the strict data privacy laws that applied to the company's European offices, the CIO brought the contracts to the company's general counsel for review.

Cloud Computing and SaaS Solutions
Cloud computing is the use of computing resources, including both hardware and software, that are made available over the Internet by a subscription-based service provider. Software as a service (SaaS) is one type of cloud computing service that provides companies with remote access to software being hosted by a third party. Companies often adopt SaaS solutions for email because doing so allows employees to access corporate email from any device connected to the Internet. In addition to providing increased mobility and accessibility, cloud-based email may reduce the costs associated with acquiring and maintaining email servers.

To stay current with the latest technology, minimize their own hardware, development and support costs, attract the widest customer base possible, vendors providing cloud-based email services often offer a standardized product with little or no customization. Given the nature of off-the-shelf SaaS solutions—a single product being offered to a large number of customers—vendor services are often provided to many customers simultaneously. Because highly negotiated contracts would make implementation and support impracticable, SaaS contracts also tend to be standardized. This does not, however, mean that companies seeking to use cloud-based email should give up on negotiating the contractual terms, especially those that may require modification to comply with data privacy laws. On the contrary, they should expect to negotiate the terms, particularly with respect to provisions assuring compliance with data privacy laws.

Cloud Computing and EU Data Privacy Laws

While moving email to a cloud provider presents a number of data privacy risks for all companies, it presents a more complicated challenge for companies with operations in both the United States and the European Union, especially if the potential cloud provider's facilities are located in the United States. The EU has implemented a comprehensive regulatory framework that, among other things, sets forth the circumstances under which personal data (encompassing a broad range of information, including name, age, gender, marital status, nationality, citizenship, veteran status, personal or business contact information—including email addresses—and identification numbers)

may be lawfully transferred to parties residing in foreign jurisdictions. In the context of cloud computing, the EU maintains that these laws are triggered when either the company or the cloud provider is located within the EU. Other laws that could potentially affect email in the cloud are the so-called blocking statutes, instituted by a number of EU member nations, which prohibit the transfer of data requested in the course of foreign legal proceedings.

Location of Data

Companies assessing the risks of migrating their email to the cloud need to know which laws will be triggered. To make that assessment, they must know where the data will be hosted. The answer, however, is not always clear. Depending on how a vendor has configured its network, a client's email could be separated and stored on multiple servers in various locations. When evaluating potential cloud providers, it is crucial that vendors disclose where a company's data will be hosted.

Use of Subcontractors

A SaaS solution consists of various components that may be beyond the control of company using the solution, such as the hardware, the operating system and the network infrastructure. However, the vendor might not be the entity that operates each of these elements. Instead, the SaaS provider may subcontract with a third party to provide one or more of them. Additionally, there are a number of services required to provide cloud solutions, including hosting, processing, transmission and security, which also may be subcontracted to third parties. Not only does the use of subcontractors make it harder to determine where the data is hosted; if not handled properly, it may also run afoul of EU data privacy laws.

Tips for Managing Risk

To properly assess the data privacy risks associated with using cloud-based email, a company with data hosted in the EU needs to know who will be handling the data and where the data will be hosted. Once the company has this information, it will be in a better position to request certain contractual terms designed to ensure compliance with EU data privacy laws.

When negotiating a contract for cloud-based email, consider the following:

- Region-specific servers: The company should require that email for EU-based operations reside on a server in the EU. Similarly, the company should require that a server be based in the United States to host all US email. Keeping all US email within the United States will make it easier for the company to comply with any applicable state or federal data privacy laws and prevent possibly subjecting that email to the blocking statutes of EU member nations.
- Identify subcontractors: The company should ask the cloud services provider for both the identity and location of any subcontractors that will be working with the company's email. EU data privacy laws require cloud providers to disclose the identity of any subcontractors that will be used to provide services in connection with a SaaS contract.
- Subcontractor agreements: Cloud providers must provide the company with assurances that all subcontractors will comply with EU data privacy laws, which can be accomplished through an agreement between the cloud provider and each subcontractor reflecting the data privacy safeguards appearing in the contract between the cloud provider and the company. Additionally, the company should have recourse for any breach caused by a subcontractor. This can be accomplished through either (1) a provision contained in the agreement between the cloud provider and the company stating that the cloud provider remains liable for any work done by a subcontractor in connection with the agreement or (2) a provision in each contract between the cloud provider and a subcontractor that names the company as

a third-party beneficiary.

- Cross-border data transfers: The European Commission has adopted model contractual clauses designed to provide adequate safeguards in the context of cross-border data transfers. If a cloud provider cannot guarantee that email will be hosted within the borders of EU member countries or if the cloud provider uses subcontractors located outside of the EU, then such model clauses should be included in the SaaS contract.

For inquiries related to this Tip of the Month, please contact Eric Evans at eevans@mayerbrown.com or Michael D. Battaglia at mbattaglia@mayerbrown.com.

Learn more about Mayer Brown's Electronic Discovery & Information Governance practice or contact Anthony J. Diana at adiana@mayerbrown.com, Eric Evans at eevans@mayerbrown, Michael Lackey at mlackey@mayerbrown.com or Edmund Sautter at esautter@mayerbrown.com.

Please visit us at www.mayerbrown.com.