Cybersecurity & Data Privacy

STRATEGIC THINKING AND PRACTICAL LEGAL ADVICE

Five Questions General Counsels Should Ask about the Security and Privacy Implications of Cloud Services

Businesses today are increasingly turning to cloud computing solutions and accumulating data in the cloud at a staggering pace. Although cloud solutions have many advantages, they also present challenges. For example, cloud providers generally do not customize the cloud environment for any particular customer's business needs given the multi-tenant nature of cloud solutions. In addition, complying with data privacy and cybersecurity regulations in the cloud environment requires special consideration.

Prudent practices dictate that customers conduct due diligence on providers and the security of their solutions. Successful and compliant use of cloud computing requires businesses to fully evaluate the nature of the data to be placed in the cloud, the associated data privacy and cybersecurity laws applicable to that data, and the structure and location of the cloud solution itself. This article describes five privacy and security-related questions that a general counsel should ask regarding cloud services.

Where Will the Data in the Cloud Environment Be Stored, Processed and Transferred?

In a traditional IT setting, a business knows where its data is processed and stored. In a cloud computing environment, however, that may not be the case. A cloud provider typically maintains the freedom to move data in order to maximize resource usage across a multi-customer base, facilitating a lower cost solution than achievable under traditional outsourcing. Accordingly, data may exist or be accessed (including remotely) from numerous locations that may change from time to time, triggering data transfer requirements. In particular, the EU General Data Protection Regulation ("GDPR") regulates the transfer of data to countries not deemed to have adequate data protection laws. Transfers of data to such countries must be accomplished through implementation of permitted regulatory measures, and the permitted means for transfer should be set forth in the cloud contract.

What Data Safeguards and Protocols Will Apply to Company Data in the Cloud?

Providers are becoming more sophisticated in understanding the need to develop cloud solutions designed to meet regulatory requirements, such as obligations under the GDPR and US data privacy laws to safeguard personal data. Similarly, the Safeguards Rule under the Gramm-Leach-Bliley Act requires that a financial institution develop a written information security plan describing how it will protect nonpublic personal information, and OCC guidance requires financial institutions to implement risk management processes for third-party relationships. Similarly, the Security Rule under the Health Insurance Portability and Accountability Act requires that covered entities implement administrative, physical and technical safeguards to protect the security of electronic protected health information. Non-governmental

organizations, such as the Payment Card Industry Data Security Standards Council, may also impose similar requirements on their members. Several states also have data security requirements. Accordingly, cloud contracts will need to address the provider's obligations to safeguard personal data in a manner that allows the customer to remain compliant.

How Will the Business Monitor the Cloud Provider's Compliance with Data Security and Privacy Protocols?

Many privacy laws and regulations require that the customer maintain the ability to monitor the performance of third party providers, such as by conducting audits. However, in many cases, a cloud provider will not—or may not be able to—offer broad audit rights, either for policy and risk reasons or because the cloud provider is relying on a web or network of data centers provided by other third parties and subprocessors. In such cases, the customer should ask the provider what types of third-party audits or certifications of their facilities they routinely obtain. Cloud computing contracts should address provider obligations to regularly conduct such audits and maintain such certifications, as well as obligations to provide audit results to the customer.

How Should the Cloud Contract Address Data Breach Notification Requirements?

In a cloud computing environment, a business is dependent on the cloud provider to notify the business if a breach occurs and to provide it with necessary information regarding the breach in order for the business to perform investigations or diligence or provide notifications as required by various laws. The customer and provider should negotiate terms and conditions around data breach notification, including what constitutes a data breach, the responsibility and liability associated with a data breach, and the timing of the notification of a breach.

What Rights Do Third Parties Have to Access Data by Means of Legal Process?

The location of data is also important for assessing the risk of third-party access through compulsory legal process. Recent cases suggest that the US government's ability to access US data stored outside of the United States through process served on a US provider is in a state of flux. On the other hand, storing data in a cloud environment may not alter the customer's obligations to produce its own documents through legal process. Location-of-data issues are further complicated by countries having passed "blocking statutes," which limit or prohibit exporting certain information outside the country. Such information may still be subject to US discovery rules if a US party has control over the information, creating a potential conflict of laws. Global companies should understand the complexities associated with responding to legal process across multiple jurisdictions for data stored in the cloud.

For more information about the topics raised in this Q&A, please contact any of the following lawyers.

Linda Rhodes
+1 202-263-3382
lrhodes@mayerbrown.com

Lei Shen
+1 312-701-8852
lshen@mayerbrown.com

Brad Peterson
+1 312-701- 8568
bpeterson@mayerbrown.com

Mayer Brown is a global legal services organization advising clients across the Americas, Asia, Europe and the Middle East. Our presence in the world's leading markets enables us to offer clients access to local market knowledge combined with global reach.

We are noted for our commitment to client service and our ability to assist clients with their most complex and demanding legal and business challenges worldwide. We serve many of the world's largest companies, including a significant proportion of the Fortune 100, FTSE 100, CAC 40, DAX, Hang Seng and Nikkei index companies and more than half of the world's largest banks. We provide legal services in areas such as banking and finance; corporate and securities; litigation and dispute resolution; antitrust and competition; US Supreme Court and appellate matters; employment and benefits; environmental; financial services regulatory and enforcement; government and global trade; intellectual property; real estate; tax; restructuring, bankruptcy and insolvency; and wealth management.

Please visit www.mayerbrown.com for comprehensive contact information for all Mayer Brown offices.