Bloomberg BNA

Daily Report for Executives™

Internet

The rush of companies seeking the efficiencies of cloud computing could engender some serious legal hangovers in the form of liability for privacy violations, if cloud clients fail to exercise due diligence, authors Alan Charles Raul and Edward McNicholas suggest.

U.S. and EU regulators are concerned enough to have recently issued guidances charting potential pitfalls that must be addressed. Raul and McNicholas pull together the essence of these advisories to help those new to the market make sure they have their bases covered.

U.S., EU Offer Guidance on Due Diligence for Cloud Computing Arrangements

ALAN CHARLES RAUL AND EDWARD R. MCNICHOLAS

Recent guidance from financial regulators in the United States and the data protection authorities in the European Union sound a note of caution about moving to the cloud without careful advance planning. The U.S. and EU authorities have focused directly on the responsibility of cloud customers to conduct diligence on cloud providers and to provide rigorous oversight of their service providers.

The guidance acknowledges that cloud computing provides enormous benefits to companies seeking efficient computing solutions. Cloud service providers can offer centralized data management to companies around the world at a fraction of the cost of traditional computing and software distribution models.[1] Not surprisingly, therefore, there has been a rapid shift of data to the cloud, throughout the private sector, and the Obama administration, with its ''cloud-first policy,'' has been a vocal proponent of migration of government data to the cloud.[2]

But the benefits are not without risks—and novel legal concerns. For example, the status of cloud providers under the Electronic Communications Privacy Act remains subject to considerable debate (for instance, when will they be deemed ''remote computing services''?). As more data moves to the cloud, there are also increasing concerns about the security of the cloud, which is largely managed by cloud providers and their subcontractors, which necessarily entails some loss of control for data owners. On the other hand,

Alan Charles Raul and Edward R. McNicholas are global coordinators of Sidley Austin LLP's Privacy, Data Security and Information Law group, based in Sidley's Washington, D.C. office. The views expressed herein are those of the authors personally and do not necessarily reflect the views of any governmental or private entity, client, or association. This article is published for informational purposes only and is not legal advice.

[1] National Institute of Standards and Technology, Special Publication 800-146, 1 (May 2012), available at http://www.nist.gov/customcf/get_pdf.cfm?pub_id=911075.

[2] Vivek Kundra, Federal Cloud Computing Strategy (Feb. 8, 2011), available at *http://www.cio.gov/documents/federal-cloud-computing-strategy.pdf*.

 ISSN 0148-8155

cloud providers may have the day-in, day-out expertise to provide security arrangements at a high common denominator.

Data owners are often faced with cloud terms and conditions that offer a one-size-fits-all (and take-it-or-leave-it) approach to privacy and security.

Yet, data owners are often faced with cloud terms and conditions that offer a one-size-fits-all (and take-it-or-leave-it) approach to privacy and security—and often involve a service provider that has significantly more bargaining power. Nevertheless, eager to avail themselves of a highly efficient and cost-effective computing solution, many companies (and individuals) have been willing to accept stock terms and conditions without being able to conduct the type of diligence typically performed in their other outsourcing arrangements of comparable importance.

U.S. Guidance on Cloud Computing for Financial Institutions

On July 10, the six U.S. federal agencies[3] that make up the Federal Financial Institutions Examination Council issued a guidance on ''Outsourced Cloud Computing,'' in which they identify cloud computing as ''another form of outsourcing with the same basic risk characteristics and risk management requirements as traditional forms of outsourcing.''[4] The four-page guidance observes that boards of directors and other senior managers of financial institutions that use cloud providers bear undiminished responsibility for ensuring that ''the third-party activity is conducted in a safe and sound manner and in compliance with applicable laws and regulations.''[5]

In following the outsourcing processes in the *FFIEC Information Technology Examination Handbook*, financial institutions should focus in particular on the following elements of the outsourcing relationship:

- **Due Diligence.** In selecting a provider, conduct due diligence paying particular attention to data classification (protection of data commensurate with its sensitivity); data segregation (preserving the integrity and confidentiality of data in storage, processing and transmission, particularly if the data is commingled with that of other cloud clients); and recoverability (disaster recovery and business continuity).
- **Vendor Management.** Ensure that the cloud provider meets contractual and regulatory requirements, particularly those that are unique to financial services.
- **Audits.** Examine the cloud provider's internal controls and rectify deficiencies.
- **Information Security.** Revise internal policies in light of the activities of the cloud provider. Tailor security to the risks presented by the outsourcing relationship.
- **Legal, Regulatory, and Reputational Considerations.** Understand how using a cloud provider overseas (or where extra-territorial transfers are foreseeable) affects legal obligations and may present reputational risks if the cloud provider is less protective of personal information.
- **Business Continuity Planning.** Examine abilities to overcome disruption in service.

EU Cloud Computing Guidance

Shortly before the FFIEC issued its guidance, the EU's Article 29 Working Party also addressed the cloud. On July 1, the Working Party issued a draft opinion on Cloud Computing, No. 05/2012,[6] which, like the FFIEC guidance, advises cloud customers to maximize oversight of cloud arrangements. Whereas the FFIEC guidance only applies to financial institutions (although it may be influential beyond the financial sector), the EU guidance applies to any cloud customer or provider subject to the EU Data Protection Directive.[7]

Before selecting a cloud provider, the Opinion advises cloud customers—''data controllers'' within the meaning of the European Data Protection Directive—to conduct a comprehensive data protection risk assessment, designed to minimize two principle risks common to many cloud arrangements:

- **Lack of Control** over personal data, manifested by lack of availability due to lack of inoperability (e.g., cloud provider's proprietary technology locks out the data controller); lack of integrity and isolation caused by sharing of resources (e.g., commingling of data of various cloud clients); lack of confidentiality due to law enforcement requests directly to the cloud provider; lack of intervenability (e.g., sub-contracting), etc.; and
- **Lack of Transparency** as to where (e.g, by transfers outside the European Economic Area (EEA)), by whom (e.g., sub-contractors or ''chain processing''), and how these data are processed.

The Opinion contains a list of 14 specific issues that the cloud customer should include in its cloud services agreement to provide the data controller with requisite ''legal certainty'' to satisfy its own obligations under the EU Data Protection Directive.[8] Among these require-

[3] The agencies that make up the FFIEC include the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corp., the National Credit Union Administration, the Office of the Comptroller of the Currency and the Consumer Financial Protection Bureau.

[4] Federal Financial Institutions Examination Council, ''Outsourced Cloud Computing'' (July 10, 2012), available at http://docs.ismgcorp.com/files/external/062812_external_cloud_computing_public_statement.pdf.

[5] *Id.* at 2.

[6] Opinion 05/2012 on Cloud Computing, 01037/12/EN, WP 196 (July 1, 2012), available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf.

[7] *Id.* at 2.

[8] These include: (1) details on the client's instructions with penalties; (2) specification of risk-based security measures, including organizational and technical measures; (3) specification of subject and time frame, extent, manner and purpose of

  DER ISSN 0148-8155

ments, the Opinion puts particular emphasis on how to handle—and legitimate— international data transfers: it suggests use of the US-EU Safe Harbor (in combination with other safeguards), the EU Model Clauses (which may require prior data protection authority approval), or binding corporate rules (BCRs) for processors.

EU Guidance on BCRs for Processors

The latter option, BCRs for ''data processors,'' builds on other recent guidance from the Working Party. On June 6, 2012, the Working Party issued a working document on setting up Processor Binding Corporate Rules, which could greatly streamline international data transfers. This important guidance would allow global companies that frequently process data for their international clients to use a set of BCRs for their actions as service providers rather than implementing ad hoc contractual data transfer agreements. With respect to the cloud, global companies (data controllers) will now be able to select a cloud provider (a data processor) whose use of BCRs legitimates storage and transfer of data in and out of cloud storage in the European Economic Area, in the United States, and elsewhere.

The Working Party's guidance on these two important and interrelated issues, cloud computing and BCRs for processors, likely stems from a desire on the part of EU regulators to provide an expedient path forward for cloud computing in Europe. The transition to cloud computing in Europe has been delayed due to concerns that cloud computing is, by its very nature, incompatible with EU Data Protection Directive, which restricts international transfers to countries outside the European Economic Area that have data protection laws that are less robust than in the EU. While the guidance will serve to ameliorate these concerns, some cloud providers may remain reluctant to tailor their services—absent sufficient financial incentive from cloud customers—to EU data protection requirements.

Guidance From the French DPA on Cloud Computing

On June 25, days before issuance of the Working Party's opinion on cloud computing, the French data protection authority, le Commission nationale de l'informatique et des libertés (CNIL), issued its own guidelines on cloud computing.[9] The CNIL guidance is largely congruent with the Article 29 Working Party's guidance, focusing on cloud-provider diligence, listing essential elements that a cloud service agreement should contain, and providing draft clauses that incorporate these elements.

In the case of certain public cloud services, the cloud provider's obligations and liabilities will be increased, the French guidance says.

According to the French guidance, the cloud provider will normally be considered a ''data processor,'' within the meaning of EU and French data protection law, who bears less data protection responsibility than the cloud customer, the ''data controller.'' Significantly, however, for certain public cloud services, where the cloud customers cannot effectively give ''instructions'' and monitor the cloud provider (as, for example, a result of non-negotiable terms and conditions), the cloud provider may be considered a joint ''data controller'' with the customer. In those circumstances the cloud provider's obligations and liabilities will be increased—and the cloud provider will have augmented incentive to provide a secure cloud.

While some cloud providers may object to diminished control in the cloud contract negotiating process, the guidelines are, overall, a boon to French companies and cloud providers alike: both will benefit from settling of expectations that will enable further migration of French data to the cloud.

the processing and types of data; (4) specification of the conditions for returning, destroying, erasing data; (5) inclusion of a confidentiality clause and limited access to data; (6) obligation on the provider's part to support the client in facilitating exercise of data subjects' rights to access, correct or delete their data; (7) statement that the cloud provider may not communicate the data to third parties, unless subcontracting is authorized by the contract (with detailed guidance on how to arrange subcontracting relationships); (8) notification of the customer of a breach; (9) obligation of the cloud provider to provide a list of locations in which the data may be processed; (10) the controller's rights to monitor and the cloud provider's obligations to cooperate; (11) informing the customer of relevant changes; (12) provision for logging and auditing of relevant processing operations; (13) notification of the client about any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited; and (14) a general obligation on the provider's part to give assurance that its internal organization and data processing arrangements are compliant with applicable law.

[9] CNIL, ''Recommandations pour les entreprises qui envisagent de souscrire à des services de Cloud computing,'' available in French at http://www.cnil.fr/fileadmin/images/la_cnil/actualite/Recommandations_pour_les_entreprises_qui_envisagent_de_souscrire_a_des_services_de_Cloud.pdf.