BNA, INC.

# PRIVACY & SECURITY LAW

BNA Employee-Owned Since 1947

REPORT



**Outsourcing Contracts**

**Cloud Computing**

## Contracting for Cloud Computing Services: Privacy and Data Security Considerations

BY TANYA L. FORSHEIT

Nearly every day, businesses are entering into arrangements to save the enterprise what appear to be significant sums on information technology infrastructure by placing corporate data ''in the cloud.'' Win-win, right? Not so fast. If it seems too good to be true, it probably is. Many of these deals are negotiated quickly, or not negotiated at all, due to the perceived cost savings. Indeed, many are closed not in a conference room with signature blocks, ceremony, and champagne, but in a basement office with the click of a mouse. Unfortunately, with that single click, organizations may be putting the security of their sensitive data (personal information, trade secrets, intellectual property, and more) at risk, and may be overlooking critical compliance requirements of privacy and data security law (not to mention additional regulations).

This article will leave aside, for the moment, the questions about whether cloud computing is new, whether it is just fancy marketing or hype, and the many forms it may take. The purpose of this article is to focus on the contract for cloud services, and privacy and data security provisions specifically. Why? Data security and privacy terms (with associated indemnities and shifting of the risk of loss) have become much more important in IT outsourcing arrangements (whether ''cloud'' or ''traditional''). Significant time, effort and expense are being expended drafting and negotiating data security and privacy terms. In fact, because of the complexity of security and privacy, and associated laws,

 ISSN 1538-3423

these terms can take more time to settle than more ''basic'' contract terms. There is significant financial risk associated with poor data security and privacy and related regulatory requirements. This risk can dwarf the value of the contract (or the savings of the contract) if favorable contract terms are not negotiated.

This article will address the following practical issues associated with outsourcing contractual IT services where sensitive data of any kind will be maintained, stored, or processed outside of dedicated company servers with a third party:

- What are some of the questions that should be asked by potential cloud customers at the Request for Proposal (RFP) and/or due diligence stage to address privacy and data security risks?

and

- What kinds of provisions should be included in the cloud computing contracts?

Needless to say, this article is not legal advice and is for informational purposes only, provides only examples that may not be appropriate to every contract, and does not exhaustively address every issue or contract provision that should be considered in a cloud contracting arrangement. Every cloud computing deal involves fact-specific considerations, and all organizations should consult with counsel in negotiating and drafting contracts with cloud service providers.

**RFPs/Due Diligence for Cloud Computing Service Arrangements** The RFP process for cloud service providers should start with consensus among all of the stakeholders within an organization—IT, legal, compliance, information security, and all of the relevant business groups. Those interested parties should jointly compile a list of questions that are relevant to a particular cloud deal. Some of those questions might include the following, from a privacy/data protection perspective:

- Does the cloud service provider have a written information security policy that maps against the requirements of applicable federal (Gramm-Leach-Bliley Act, Health Insurance Portability and Accountability Act, etc.) and state (Massachusetts, Nevada, etc.) data security laws and any applicable industry standards (International Organization for Standardization, National Institute of Standards and Technology, Payment Card Industry Data Security Standard (PCI DSS), Federal Information Security Management Act)?
- Has the cloud service provider had an independent third party audit of its security? (Obtain a copy of any audit reports.)
- What does the cloud provider's form contract provide in terms of privacy and data protection? (Obtain a copy.)
- What kind of data will be stored, processed, and/or maintained in the cloud?
- Where do the data subjects reside?
- Where will the data be stored?
  - Where are the servers?
  - Will the data be transferred to other locations, and if so, when, where, and under what circumstances?
  - Can certain types of data be restricted to particular geographic areas?
  - What is the compliance plan for cross-border data transfers?
- Has the cloud service provider experienced any data security breaches involving the services in question that have required notification to cloud service clients? What were the circumstances of those breaches? How many records were compromised? Did the cloud service provider cover the client's out-of-pocket expenses associated with the breach and indemnify the client for any claims associated with the breach?

Of course, there are numerous additional questions that may be relevant depending on the nature of the cloud service at issue, but the foregoing provides a number of ideas to start building an appropriate checklist for RFPs and due diligence inquiries.

**Privacy and Data Security Contractual Provisions** In all likelihood, any cloud services vendor selected by an organization, whether a giant IT service provider with decades of history, or a small start-up cloud operation, has a form contract. Most form contracts will not address any or all of the crucial privacy and data security issues, or will gloss over them. Customers should carefully review and revise these form agreements, and should insist on special protections where necessary to alleviate risk. Indeed, depending on the sensitivity and volume of the data being put in the cloud, there are some cases where a potential cloud customer should be prepared to walk away, or to take its business to another vendor, in the absence of sufficient protection.

Following is a description and sampling of some of the important privacy and data security provisions in cloud computing contractual arrangements. This list is not meant to be exhaustive, and all cloud customers should consult with counsel in negotiating and drafting such contracts.

- ***Scope of Information Protected***

A cloud customer should consider the scope of sensitive information covered by the contract's privacy and data security provisions. It may make more sense, from an information governance perspective, to require security for *all* kinds of sensitive information and systems, not just personally identifiable information (PII). The way to address this in a contract is to define ''Information'' or ''Sensitive Information'' to address a broad swath of data, including, for example, any data or information (whether in electronic or non-electronic form) in the care, custody or control of the service provider or a third party on the service provider's behalf: (a) provided to the service provider by the customer, a third party on behalf of the customer or the customer's customers, clients or employees; or (b) created, stored, processed or transmitted as a result of the service provider's rendering of services pursuant to the agreement, including without limitation, personally identifiable information (separately defined to include any information from which an individual may be identified), the customer's confidential or proprietary information, metadata and the customer's intellectual property or trade secrets.

- ***Definition of Security***

A good definition of ''security'' can make a cloud service provider contract much more succinct, particularly for purposes of those sections focused on a cloud provider's responsibility to provide ''reasonable security'' (see discussion below). A definition of ''security'' might include a provider's technological, physical, administrative and procedural safeguards, including but not lim-

  PVLR ISSN 1538-3423

ited to policies, procedures, standards, controls, hardware, software, firmware and physical security measures, the function or purpose of which is, in whole or part, to: (1) protect the confidentiality, integrity or accessibility of information (as defined in the agreement) and service provider systems; (2) prevent the unauthorized use of or unauthorized access to service provider systems; or (3) prevent a breach or malicious code infection of customer systems.

■ ***''Reasonable Security''***

Most federal and state data security regulations require that a company ''[t]ak[e] reasonable steps to select and retain third-party service providers that are capable of maintaining appropriate security measures to protect such personal information consistent with'' those regulations, and ''[r]equir[e] such third-party service providers by contract to implement and maintain such appropriate security measures for personal information.'' Massachusetts 201 CMR 17.03(2)(f). *See also* California Civil Code § 1798.81.5 (''[a] business that discloses personal information about a California resident pursuant to a contract with a nonaffiliated third party shall require by contract that the third party implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure''); GLB Act Safeguards Rule, 16 C.F.R. § 314.4(d) (''[t]ak[e] reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue; and . . . [r]equir[e] your service providers by contract to implement and maintain such safeguards).

''Reasonable security'' should be a floor for such contracts, not a ceiling. There are many potential variations on a ''reasonable security'' provision. At a minimum, a service provider should agree that, beginning on the effective date of the agreement and continuing as long as the service provider controls, possesses, stores, transmits or processes information (as defined in the agreement), the service provider shall employ and maintain reasonable security (also as defined in the agreement) to: (1) ensure that all information is protected from unauthorized use, alteration, access or disclosure, and to protect and ensure the confidentiality, integrity and availability of information; (2) prevent unauthorized access and unauthorized use of, and ensure the availability of service provider systems; and (3) prevent a breach or malicious code infection of customer systems.

Beyond providing ''reasonable security,'' a provider should agree that ''security'' will be consistent with all applicable privacy and data security laws and regulations and relevant industry standards. A cloud customer may want the cloud service provider to separately represent and warrant that it will adhere to the requirements of all privacy and data security laws and regulations, and will be responsible for the security of service provider systems and any information (defined in the agreement) that it controls, possesses, processes, stores or transmits.

Further, a cloud user may want to require specific controls by contract (e.g., physical and electronic access controls, secure user authentication protocols, firewall protection, malware protection, use of encryption (with details as to the level of encryption for particular kinds of data), immediate termination of access for terminated employees, assessment, monitoring and auditing procedures, and/or annual assessments and reports on safeguards).

■ ***Restrictions on Use and Disclosure of Sensitive Information***

It is imperative that a cloud customer require a cloud service provider to refrain from using any information (as defined in the agreement) it receives for purposes other than carrying out the services described in the agreement. Further, the contract should include controls to limit a service provider's ability to share sensitive information with any service provider, subcontractor, vendor, or other third party unless it has received prior written consent from the customer or such access is specifically allowed under the agreement. In any event, prior to sharing such information, a cloud service provider should be required by contract to contractually impose on its own service providers, subcontractors, vendors, and other third parties the same or substantially similar contractual duties imposed on the provider itself in the primary agreement.

■ ***Audit Rights***

The contract should provide a cloud customer with the right to assess and audit the provider's ''security'' (as defined in the agreement discussed above) and compliance with applicable privacy and data security laws and regulations at least once per year during the term of the agreement, after any actual or reasonably suspected security breach, and if the customer has any reason to be concerned that the vendor is not providing ''reasonable security'' or is otherwise not complying with law.

■ ***Definition of Security Breach (or Security Incident)***

Some cloud providers may structure their contracts to limit the definition of security breach to a breach of their security obligations under the agreement itself. Such a definition may be too narrow from the customer's perspective. Such a customer may want to define a security breach or incident to include any actual or reasonably suspected unauthorized use of or access to service provider systems or access or theft of information (as defined in the agreement), an inability to access those systems or information (as defined in the agreement) due to a malicious use, attack or exploitation of information or systems, unauthorized use of information by a person for purposes of theft, fraud or identity theft, unauthorized disclosure or alteration of information, and/or transmission of malicious code. There are numerous variations on what a security incident or breach might involve depending on the nature of the service provided.

■ ***Reporting in the Event of a Breach***

Although cloud providers are required by existing state laws, and by the Health Information Technology for Economic and Clinical Health Act, to notify a data owner in the event of a security breach, the contract should also spell out breach notification procedures. Such a provision might require a service provider to conduct an investigation of the reasons for and circumstances surrounding the breach; use best efforts and take necessary actions to prevent, contain, and mitigate the impact of the breach; provide notice to the customer (by phone and/or in writing) within a set time frame (hour or days) after discovery of a breach; collect and preserve evidence concerning the breach, including documentation regarding incident response and remedial actions taken (meeting reasonable expectations of forensic admissibility); and, if the customer so requests,

provide notice to individuals whose information may have been compromised.

■ ***Preservation, Return, and Secure Disposal of Information; Control and Access/Authentication***

For purposes of meeting evidence preservation requirements, and discovery obligations in litigation and government investigations, it may be important for a cloud services contract to require that a cloud provider preserve information and provide the customer with access to the information in the form in which it is maintained in the ordinary course of business, sometimes on short notice. Of course, like other outsourcing agreements, cloud contracts should provide for return and/or secure disposal of the information in accordance with the customer's directions.

■ ***Indemnification***

Indemnification in the event of a security breach caused by a cloud provider and/or a provider's breach of applicable privacy laws and regulations might be one of the most important provisions in a cloud services agreement. Many service providers do not include such indemnification provisions in their form contracts.

Such an indemnification provision should cover, in addition to fees and expenses incurred in connection with claims and litigation and fines and penalties paid to third parties, expenses associated with responding to a breach even in the absence of a claim or lawsuit, such as expenses incurred to provide notice to customers, employees, law-enforcement agencies, regulatory bodies or other third parties; to investigate, assess or remediate a breach; to retain a call center and/or public relations consultants; to provide credit monitoring services to individuals affected by a breach; and to respond to government investigations.

■ ***Limitations of Liability***

All potential cloud users must carefully review the terms of cloud provider service agreements when it comes to limitations of liability. Although it is common for an outsourcing partner to accept unlimited liability in the event of a breach of traditional business confidential information (e.g., trade secrets and confidential financial information), some cloud providers and other outsourcing partners have carved ''personal information'' out of the definition of ''confidential information'' for this purpose. It is reported that some services providers have agreed to unlimited liability in the event of a breach (*see, e.g.*, Patrick Thibodeau, ''Microsoft Office 2010 Throws Down Google Gauntlet, Contract terms, not features, may have major role in Google Apps vs. Office cloud decisions,'' PC World, April 8, 2010). However, many service providers may attempt to cap their liability in the event of a breach (sometimes attempting to limit liability to fees paid under the agreement itself).

Of course, the financial risk associated with a security breach of data in the cloud may dwarf the fees paid by a customer under the contract. In order to assess the true risk in the event of a breach, a cloud customer must consider how many individuals might have personal information in the cloud (including employees, customer, and third party individuals who have entrusted their information to the customer). The Ponemon Institute has estimated that a breach can cost $204/individual (9 PVLR 202, 2/1/10). But a cloud customer must also keep in mind that the reputational damage associated with a breach can be very difficult to quantify and can exceed the economic damages.

In the event that a cloud service provider is unwilling to agree to unlimited liability for any security breach, one possible approach is for a customer to seek unlimited liability for any breach caused by an action of the cloud service provider, whether willful or negligent.

■ ***Compliance with Data Protection Laws Based on the EU Data Protection Directive/Restrictions On and/or Compliance Mechanisms for Cross-Border Data Transfers***

Where a customer furnishes PII to a cloud provider that originates from a member country of the European Union, the European Economic Area, Switzerland, Russia, or another jurisdiction with data protection laws based on the EU Data Protection Directive (95/46/EC), it is especially important that the cloud provider certify in the contract its compliance with national laws based on the Directive.

If the cloud provider is a processor as defined under the Directive, it should agree to process the PII only according to the customer's instructions; the provider should also agree to take appropriate technical and organizational measures to protect the PII against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access. To the extent that the cloud provider transfers the PII to the United States, the provider should state in the contract that it has certified to the U.S. Department of Commerce its compliance with the ''Safe Harbor Privacy Framework'' accepted by the European Union and Switzerland, and that it will maintain its certification during the period in which it processes PII from the customer. The cloud provider should further represent that it will fully comply with the terms of that certification, including compliance with the ''Onward Transfer'' principle of Safe Harbor with respect to any subsequent transfers of the PII to countries other than the United States. Alternatively, in lieu of Safe Harbor certification, a cloud provider might represent in the contract that it has obtained approval for Binding Corporate Rules (BCRs) to protect PII transferred from each relevant jurisdiction and will maintain such BCRs during the period in which it processes PII from Customer, or that it will cooperate with the customer to prepare and execute any required international data transfer agreement with EU-approved Standard Contract Clauses.

## Conclusion

Organizations considering placing sensitive data in the cloud need to carefully consider the privacy and data security risks associated with such an outsourcing arrangement. As explained above, the RFP, due diligence, and contract negotiation process are crucial in identifying, assessing, and addressing those risks. Where sensitive information is at issue, no organization should rush into cloud computing deals based on perceived cost savings without evaluating the risks and putting in place appropriate contractual protections.

  PVLR ISSN 1538-3423