ADAMS AND REESE LLP

ISO Adopts Standard for Privacy in the Cloud

By Jack Pringle and Jaimmé Collins
Attorneys, Adams and Reese LLP

The use of public cloud computing services- broadly defined as contracting with another company for the provision of computing resources (networks, storage, applications, and services), offers many potential benefits for businesses, among them economies of scale, lower capital costs, and improved accessibility.

At the same time, the nature of cloud computing services presents a number of legal and compliance challenges for businesses and cloud services providers alike. For example, numerous data protection laws require businesses to safeguard personal information. These data protection laws – such as statutes based on the European Union Directive 95-46 (the "EU Data Protection Directive) -- often limit or restrict the international transfer of sensitive information, and require organizations controlling or processing data to execute Model Contract Clauses or Binding Corporate Rules in order to affect cross-border data transfers.

When a business (the customer) agrees to allow a cloud services provider to process personal information (e.g. collect, store, use, and dispose of that information), the customer continues to be bound by those data protection and transfer requirements. Accordingly, a business entrusting personal information to a cloud services provider retains the responsibility to ensure that the cloud services provider adequately protects personal information and only transfers sensitive data in compliance with applicable law.

Similarly, data protection laws governing how personal information can be processed are not necessarily uniform from country to country, creating additional challenges for those customers and cloud services providers operating in more than one jurisdiction. And although there are a number of standards addressing information security generally- such as International Standards Organization (ISO) 27001 and 27002- the absence of a single privacy standard particular to cloud services makes assessing data protection compliance (via audit or otherwise) problematic. In fact, the European Commission's 2012 report "Unleashing the Potential of Cloud Computing in Europe" cited the lack of such a standard as a hindrance to the widespread use of cloud computing in Europe.

With an eye toward establishing a "common compliance framework" for cloud services providers that could apply across jurisdictions, on August 1, 2014 ISO issued a standard- ISO 27018- for protecting personal information in the cloud. ISO 27018 sets out the following objectives:

- Help cloud services providers comply with their legal, statutory, regulatory and contractual obligations applicable to the processing of PII;
- Allow cloud services providers to be transparent so that their customers can select cloud-based services;
- Help a cloud service customer and the cloud services provider to enter into a contractual relationship; and
- Give cloud services customers a mechanism to audit their cloud services providers, given the difficulties associated with doing so in a multi-party cloud environment.

In establishing its compliance framework, ISO 27018 considers some of the unique aspects of cloud services (for example the distributed nature of cloud service risk and a contractual relationship between a cloud services provider and its customer), and supplements the information security framework provided by ISO 27001 and ISO 27002 with specific guidance and controls applicable to cloud services.

Some key personal information protection requirements ISO 27018 establishes for cloud services providers include:

- Process information only as instructed by the customer, and provide the customer with access to information necessary to confirm same;
- Never process personal information for advertising and marketing purposes without the express consent of the customer. Requiring consent as a condition of service is prohibited;
- Make clear in its contractual arrangements with the customer that it will a) reject requests for personal information that are not legally binding; b) consult the customer when legally permissible before making any disclosure of personal information; and c) accept any requests for disclosures of personal information authorized by the customer;
- Notify the customer of any request for disclosure of personal information by a law enforcement authority unless that disclosure is otherwise prohibited;
- Disclose the use of any sub-contractors to the customer prior to using them, as well as material information (names of sub-contractors, countries in which sub-contractors

process information, how sub-contractors will meet or exceed the information security obligations of the cloud services provider) about the sub-contractor(s);

- Notify the customer promptly of any unauthorized access to personal information or loss, disclosure or alteration of personal information;
- Help the customer meet its obligations in the event of a data breach;
- Implement a policy for the return, transfer, and disposal or personal information and make that policy available to the customer; and
- Require all individuals with access to personal information to be bound by a confidentiality agreement.

A cloud services provider has the opportunity to gain certification under ISO 27018 through a review of its systems and policies, a compliance audit by an accredited certification body, and subsequent periodic (typically annual) third-party reviews. Customers and data controllers may use ISO 27018 as a benchmark for meeting their legal obligations, contractual obligations and business objectives applicable to the protection of personal information.