MORRISON | FOERSTER

Morrison & Foerster Client Alert

27 March 2015

Cloud Data Security Standards Reach New Heights?

By Sue McLean and Alex van der Wolk

Issues of data privacy and security are central to most cloud contract negotiations. While cloud service providers may be willing to take responsibility for the integrity of their networks, accepting obligations in relation to data privacy and security typically requires more discussion. However, that discussion may now become a little easier as a result of the introduction of ISO/IEC 27018, the first international voluntary standard that focuses specifically on data security in the public cloud. Although ISO/IEC 27018 was published back in July 2014, it received a significant boost recently when Microsoft announced that it has become the first major cloud services provider to adopt the standard.

In this Alert, we outline some of the key requirements of ISO/IEC 27018 and consider what its adoption may mean for the cloud sector.

As we discussed in our recent Alert, Negotiating Cloud Contracts, the cloud computing market is evolving rapidly. And while many of the key issues remain the same, in some areas service providers' commercial offerings are becoming more flexible. In particular, we are seeing an increased willingness by providers to negotiate on certain issues and to provide assurances that they take seriously regional privacy and security concerns. So, what does ISO/IEC 27018 add?

ISO/IEC 27018

To give it its full name, ISO/IEC 27018 is a "Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors". It is published by the ISO (International Organization for Standardization) which is an independent, non-governmental membership organization and the world's largest developer of voluntary international standards.

Because data privacy and security laws and regulations vary from jurisdiction to jurisdiction, the ISO acknowledges that compliance can be challenging for cloud service providers. Accordingly, this new international standard is intended to provide a common compliance framework for public cloud service providers, particularly those operating in a multinational market.

UNITED STATES

California
Tiffany Cheung (415) 268-6848
Kimberly R. Gosling (858) 314-5478
Rebekah Kaufman (415) 268-6148
Christine E. Lyon (650) 813-5770
David F. McDowell (213) 892-5383
Purvi G. Patel (213) 892-5296
Andrew Serwin (858) 720-5134
Stephanie Sharron (650) 813-4018
William L. Stern (415) 268-7637
Nancy R. Thomas (213) 892-5561
David M. Walsh (213) 892-5262

New York
Cindy Abramson (212) 336-4178
Melissa Crespo (212) 336-4354
John F. Delaney (212) 468-8040
Michael B. Miller (212) 468-8009
Sotirios Petrovas (212) 336-4377
Suhna N. Pierce (212) 336-4150
Marian Waldmann Agarwal (212) 336-4230
Miriam H. Wugmeister (212) 506-7213

Washington, D.C.
Patrick Bernhardt (202) 887-8771
L. Richard Fischer (202) 887-1566
Adam J. Fleisher (202) 887-8781
Libby J. Greismann (202) 778-1607
Julie O'Neill (202) 887-8764
Cynthia J. Rich (202) 778-1652
Nathan David Taylor (202) 778-1644

EUROPE

Berlin
Hanno Timner 49 30 72622-1346
Lokke Moerel 44 20 79204054
Alex van der Wolk 44 20 79204054

Brussels
Karin Retzer 32 2 340 7364
Alja Poler De Zwart 32 2 340 7360

London
Susan McLean 44 20 79204045

ASIA

Beijing
Paul D. McKenzie 86 10 5909 3366

Hong Kong
Gordon A. Milner 852 2585 0808

Singapore
Daniel P. Levison 65 6922 2041

Tokyo
Toshihiro So 81 3 3214 6568
Yukihiro Terazawa 81 3 3214 6585

The new ISO/IEC 27018 forms part of the ISO 27000 family of standards. These are a set of standards specifically aimed at helping organizations to keep their information assets secure. ISO/IEC 27001 is the best-known of these standards and provides requirements for an information security management system ("ISMS"). Certification to ISO/IEC 27001 is possible but not obligatory. ISO/IEC 27002 is a related code of practice which sets out information security controls designed to be used by organizations that are implementing an ISMS based on ISO/IEC 27001. Neither ISO/IEC 27001 nor 27002 is specific to the cloud sector.

The new ISO/IEC 27018 standard takes into account the specific risk environment which applies to cloud service providers, and it builds on the security controls detailed in ISO/IEC 27002. The new standard augments ISO/IEC 27002 in two ways: (i) it provides additional guidance on how to implement the existing controls set out in ISO/IEC 27002, and (ii) it introduces additional controls that are specific to cloud services.

As ISO/IEC 27018 is international in scope, it does not reflect the data privacy law of any one jurisdiction.

Note, for example, that the standard refers to PII and not "personal data" (which is the term used in EU data protection law) or "personal information" (which is the term used in certain other jurisdictions, *e.g.*, Australia). The standard acknowledges that "PII is sometimes referred to as personal data or personal information".

In terms of European data protection law, broadly speaking the provisions of ISO/IEC 27018 are consistent with the spirit of the guidance on cloud computing published by the EU's Article 29 Data Protection Working Party on 1 July 2012 ("WP29 Opinion") and related country-specific guidance on data security (*e.g.*, the UK ICO's guidance on cloud computing 2012).

However, it's important to point out that the new ISO data security standard is firmly aimed at cloud service providers (*i.e.*, PII/data processors), not customers (*i.e.*, PII/data controllers). ISO/IEC 27018 states that most of the controls and guidance in the standard would also apply to a PII/data controller but acknowledges that the PII/data controller will, in most cases, be subject to additional legal obligations.

OBJECTIVES

ISO/IEC 27018 has the following objectives:

- to help public cloud service providers to comply with applicable obligations when acting as a PII processor, whether such obligations fall on the PII processor directly or through contract;
- to enable public cloud PII processors to be transparent so that customers can select well-governed cloud-based PII processing services;
- to assist cloud service customers and public cloud PII processors entering into a contract; and
- to provide customers with a mechanism for exercising audit and compliance rights and responsibilities in cases where individual cloud service customer audits of data hosted in a public cloud might be impractical technically and might increase risks to those physical and logical network security controls in place.

KEY REQUIREMENTS

The new standard includes the following key requirements for cloud service providers:

- only process PII according to the instructions of the cloud services customer as detailed in the contract;
- only process PII for marketing and advertising with the customer's express consent. Such consent must not be a condition of receiving the service;
- where individual customer audits are impractical or may increase risks to security, make available to prospective customers evidence of an independent audit of the provider's processing operations. This must be done prior to entering into and for the duration of the contract;
- provide means for the customer to comply with its obligations in terms of subject access requests;
- promptly notify the customer in the event of unauthorised access to PII or any event resulting in data loss or breach. Include data breach provisions in the contract, including in terms of notification and record keeping;
- notify the customer of any legally binding request for disclosure of PII by law enforcement, where permitted by law;
- have policies in place in respect of the retention, return, transfer and disposal of PII. A minimum retention period of five years is recommended in the absence of specific legal or contractual commitments;
- clearly identify in the contract the allocation of responsibilities between the cloud services provider, any sub-contractor(s) and the customer, taking into account the type of cloud service in question;
- make staff aware of the possible consequences of any information security breach and ensure a confidentiality agreement is in place between the provider and its employees and agents;
- disclose details of sub-contractors used to process PII to customers before use, including in terms of location of processing and extent of flow-down obligations;
- specify and document those countries in which PII may be stored. Where specific contractual requirements apply to the international transfer of data such as Model Contract Clauses, Binding Corporate Rules, etc., these should be identified;
- inform the customer of any intended changes to sub-contracting and specific contractual arrangements on a timely basis so that the customer has the ability to object or terminate the contract.

To be certified under ISO/IEC 27018, a cloud services provider needs to be audited by an accredited certification body. Cloud customers can verify a provider's compliance with the standard via the provider's certificate of conformity.

On 17 February 2015, Microsoft announced that it has become the first major cloud services provider to adopt ISO/IEC 27018. Microsoft's compliance to the new standard in respect of Microsoft Azure, Office 365 and Dynamics CRM Online has been certified by the British Standards Institute (BSI). Another independent body, Bureau Veritas, has provided certification in respect of Microsoft Intune.

WHAT DOES THIS MEAN FOR CLOUD SERVICE CUSTOMERS?

Certification against ISO/IEC 27001 and compliance with ISO/IEC 27002 are generally considered best practice in terms of information security and certain customers will mandate that their providers meet these standards. In the same way, cloud service customers may begin to require that cloud service providers comply with this new voluntary standard for cloud.

If a cloud services provider has achieved certification against ISO/IEC 27018, the customer will want to ensure that an obligation to maintain the certification is included in the contract. Even where a cloud services provider has not achieved certification, a customer may wish to include in the contract an obligation on the provider to comply with the requirements set out in the standard.

Of course, as mentioned above, the fact that a cloud services customer uses a cloud services provider that is certified against the new standard will not ensure that the cloud services customer is compliant with its legal obligations. Customers still need to ensure that they comply with all applicable privacy laws and regulations in the applicable territories when appointing a cloud services provider. Customers should still observe relevant applicable guidance (*e.g.*, in the EU, the WP29 Opinion and any related country-specific guidance on data security such as the UK ICO's guidance on cloud computing) when embarking on any cloud services project. In the same way, the new standard may be useful to customers in terms of identifying any specific information security controls that may be appropriate to include in the information security requirements detailed in the contract.

For a broader discussion of privacy in the cloud, please read our previous alert, "Privacy in the Cloud: A Legal Framework for Moving Personal Data to the Cloud".

CONCLUSION

Privacy and security risks have always been a key concern for customers considering using cloud services, particularly those customers in heavily regulated sectors such as financial services. Recent cyber attacks on cloud service providers and reports of cloud service providers being implicated in government surveillance have done nothing to help build trust in the public cloud.

Until now, although ISO/IEC 27018 has been seen as a positive step towards more uniform cloud privacy and security practices, it existed somewhat in a vacuum. It really needed adoption to give it a stamp of credibility. Microsoft's decision to adopt ISO/IEC 27018 could well spur other cloud service providers into action. However, it remains to be seen whether ISO/IEC 27018 will become the de facto standard employed by providers industry-wide.

About Morrison & Foerster:

We are Morrison & Foerster — a global firm of exceptional credentials. Our clients include some of the largest financial institutions, investment banks, Fortune 100, technology and life science companies. We've been included on *The American Lawyer's A-List* for 11 straight years, and *Fortune* named us one of the "100 Best Companies to Work For." Our lawyers are committed to achieving innovative and business-minded results for our clients, while preserving the differences that make us stronger. This is MoFo. Visit us at www.mofo.com.

Morrison & Foerster has a world-class privacy and data security practice that is cross-disciplinary and spans our global offices. With more than 60 lawyers actively counseling, litigating, and representing clients before regulators around the world on privacy and security of information issues, we have been recognized by *Chambers* and *Legal 500* as having one of the best domestic and global practices in this area.

For more information about our people and services and the resources we offer such as our treatise setting out the U.S. and international legal landscape related to workplace privacy and data security, "*Global Employee Privacy and Data Security Law,*" or our free online Privacy Library, please visit our practice page and follow us on Twitter @MoFoPrivacy.

Because of the generality of this update, the information provided herein may not be applicable in all situations and should not be acted upon without specific legal advice based on particular situations. Prior results do not guarantee a similar outcome.