GT GreenbergTraurig

ADVISORY

Privacy and Data Security | November 2014

ISO 27018 – Data Protection Standards for the Cloud

In July 2014, the International Organization for Standardization (**ISO**) and International Electrotechnical Commission (**IEC**) published ISO/IEC 27018 (**ISO 27018**),[1] a code of practice that sets forth standards and guidelines pertaining to the protection of data consisting of "personally identifiable information" (**PII**) processed by public cloud service providers.[2]

Background to the Release of ISO 27018 – Overcoming Data Protection Challenges in the Cloud Market

In recent years, business enterprises and consumers have shifted significant data and functions from local servers, hardware and devices to the "cloud." This migration is anticipated to increase exponentially, with forecasters predicting significant increases in cloud storage and traffic, as well as in revenue earned by cloud service providers.[3] Notwithstanding the anticipated extent of such migration, challenges remain to customers' continuing adoption of and migration to cloud services, particularly with respect to personal data or PII. Chief among these challenges is data security, as some customers have indicated a concern regarding a "loss of control" over data removed from their premises to a public cloud services provider.[4] Governmental authorities and regulatory bodies, such as the European Commission, have cited concerns over the need to address data security concerns for the purpose of facilitating continuing market acceptance of cloud services.[5] The United States Senate recently introduced legislation relating to the privacy of the contents of electronic communications, partly in response to efforts by the U.S. government to obtain copies, pursuant to a federal warrant issued to a U.S. provider, of e-mails stored on a server in Ireland.[6]

Cloud services involve the migration, transmission and storage of data across infrastructure that can span multiple jurisdictions and countries, particularly as cloud service providers seek to optimize hardware and other assets that comprise their cloud network. Various sets of laws and regulations from these jurisdictions, in addition to contractual requirements, apply to PII. Accordingly, public cloud services providers who process PII seek to demonstrate to customers that their services comply with applicable laws, regulations and additional requirements. In response to the foregoing challenges, the release of ISO 27018 is intended to facilitate the following objectives:[7]

- *Transparency* –

Cloud service customers can have greater information, tools and guidelines available to them for the purpose of selecting appropriate cloud services involved in processing PII;

- *Standardized and negotiated contract terms and policies* –

Recognizable standards and guidelines should aid in the development and negotiation of cloud service contracts and service level agreements governing the rights and obligations of cloud service providers and their customers with respect to the protection of PII;

- *Compliance* –

Cloud service providers should have available to them a framework in which to structure and implement controls and processes for compliance with various law, regulations, policies and contractual obligations; and

- *Auditable standards* –

The development and availability of standards based upon the information security categories and controls of 27018 (and ISO 27002) could enable public cloud service providers to demonstrate to customers their compliance with applicable laws, regulations and data protection standards, as well as provide practical and effective substitutes for individual customer audits.

Framework for the Introduction of Cloud Specific Guidelines

Current standards for data security, such as ISO 27001/27002, involve the protection of a party's own information assets, and also generally address security for physical locations where data is accessed and stored; whereas ISO 27018 relates to the protection of information assets entrusted to another party (a public cloud service provider processing PII).[8] ISO 27001 consists of a framework relating to the management of information security risks, and lays out specific mandatory steps that an organization can take to implement an information security management system. ISO 27002 sets forth a broad range of information security controls and objectives, from which organizations adopting ISO 27001 are free to choose, modify or supplement based upon their own assessment of applicable information security risks.

ISO 27018 explicitly builds upon and augments ISO 27002 by addressing each of the controls set forth in ISO 27002.[9] Each control category from ISO 27002 is evaluated and elaborated upon to the extent appropriate to address standards for protecting information assets entrusted to another party (a public cloud service provider processing PII) by cloud service customers, and new control categories and objectives have been appended at Annex A of ISO 27018. Similar to its options relating to the evaluation and selection of appropriate ISO 27002 controls, an organization implementing ISO 27001 would have the option to select, modify, supplement or disregard ISO 27018 controls and objectives based upon its own circumstances and information security risks and requirements relating to the processing of PII.

Specific ISO 27018 Guidelines for Data Protection

As a guiding principle, ISO 27018 standards and guidelines facilitate the retention by the cloud service customer of authority to determine the scope of any use and handling of its PII. The following controls and implementation guidelines set forth in ISO 27018 as generally applicable to cloud service providers processing PII supplement the controls set forth in ISO 27002:[10]

- *Customer and end user control rights:*
  - A cloud service customer should have the means to enable the individual to whom PII relates to access, correct and/or erase such PII;
  - PII should not be processed for any purpose except pursuant to the instructions of the cloud service customer;
  - PII should not be used for marketing or advertising purposes without the customer's consent;
  - Temporary files and documents associated with PII processing should be erased or destroyed by a cloud services provider within a specified period;
- *Restrictions on disclosure to or access of 3rd parties to PII:*
  - Law enforcement requests for disclosure of PII must be disclosed to a cloud service customer (unless such disclosure is prohibited by law);
  - Other requests for disclosure of PII should be rejected except to the extent authorized by a cloud service customer;
  - Data relating to disclosures of PII to third parties should be recorded;
  - Subcontractors should be disclosed in advance by a PII processor;
  - Unauthorized access to PII or processing equipment or facilities resulting in the loss, disclosure or alteration of PII should be disclosed to a cloud service customer;
  - Anyone (including cloud service provider employees) associated with the processing of PII should be subject to a confidentiality obligation;
- *Treatment of Media Containing PII:*
  - A number of additional restrictions should be maintained for information security purposes, with respect to, *inter alia*, the creation of hard copy materials displaying PII, data recovery or restoration efforts, PII stored on transportable media, transmission of PII over public networks, and user IDs for access to stored PII.

In addition to the foregoing, ISO 27018 sets forth guidance and information with respect to numerous control categories previously addressed by ISO 27002.[11]

The Future of Data Protection under ISO 27018

The release of ISO 27018 responds to an ongoing effort by information security regulatory bodies, such as the European Commission, to establish a uniform set of standards applicable to public cloud services. Various constituents, such as regulators and parties subject to their jurisdiction (*e.g.*, cloud service providers and enterprise customers), maintain as an objective the development of uniform personal data protection standards that facilitate compliance with laws, regulations and data protection standards across multiple jurisdictions. It is envisioned that such standards will drive increasing customer acceptance of cloud services for the processing of personal data.

The degree to which ISO 27018 gains acceptance in the cloud services market and the degree to which auditable standards arise from ISO 27018 remain to be seen. Given that the drafters of ISO 27018 have

integrated the controls and objectives of the widely-recognized ISO 27001/27002 framework into ISO 27018, and the significance of the bourgeoning cloud market's need to address compliance issues relating to personal data, ISO 27018 is likely to receive increased attention from industry participants in the coming years. However, both ISO 27002 and ISO 27018 set forth an optional set of controls and guidelines for processors of PII. As such, customers should closely examine the controls and measures implemented by a cloud services provider, even in the case of a provider who has achieved certification pursuant to a recognized information security or data protection standard. The particular controls adopted or discarded by a provider based upon ISO 27018 (in addition to the fact of a provider's certification under an applicable data protection standard) may be of particular interest to a customer, depending upon the laws, regulations and contractual and policy obligations to which the customer may be subject.

---

[1] ISO/IEC, Information technology – Security techniques – Code of Practice for protection of personally identifiable information (PII) in public clouds acting as PII processors, 2014 (ISO 27018).

[2] ISO 27018 (§ 3.2) defines PII as any information that can be used to identify an individual to whom the information relates, or is or might be directly or indirectly related to such individual. A number of functions constitute the "processing" of PII, including, *inter alia,* the collection, storage, alternation, retrieval, disclosure, anonymization or dissemination of PII, or the making available, deleting or destroying PII. ISO 27018 §3.6.

[3] Cisco Global Cloud Index: Forecast and Methodology 2012-2017, pages 1, 8, 25 (2013); *see also* KPMG International, Breaking through the cloud Adoption Barriers – KPMG cloud Providers Survey, page 2 (2013) (KPMG Report).
A Forrester's report indicates that public cloud business services will grow from $4.7 billion to $14 billion in 2020. Public cloud platforms are anticipated to generate $44 billion in revenue by 2020 compared with just $4.7 billion last year, a compound annual growth rate of 38 percent.

[4] KPMG Report, *supra* at page 11.

[5] European Commission, Communication from the Commission to the European Parliament et al.: Unleashing the Potential of Cloud Computing in Europe (2012)

[6] Law Enforcement Access to Data Stored Abroad Act, S. 2871 – 113th Congress (Sept. 18, 2014). *See also* John Ribeiro, "Senate Bill Would Limit Access to Emails Stored Abroad," *ComputerWorld* (Sept. 18, 2014).

[7] ISO 27018 §0.1.

[8] *Id.* at §0.2.

[9] *Id.* at §0.4. ISO 27002 controls are incorporated into ISO 27018 by reference.

[10] *Id.* at Annex A.

[11] *Id.* at §§5-18.

This *GT Alert* was prepared by **Jonathan A. Beckham**, with assistance from **Audrey T. Borisov**, **Kedrick N. Eily**, and **Angela F. Ramson**. Questions about this information can be directed to:

- Jonathan A. Beckham | +1 703.903.7534 | beckhamj@gtlaw.com
- Kemal Hawa | +1 703.749.1379/+1 202.331.3119 | hawak@gtlaw.com
- Alan N. Sutin | +1 212.801.9286 | sutina@gtlaw.com
- Or your Greenberg Traurig attorney

Albany
+1 518.689.1400

Amsterdam
+31 (0) 20 301 7300

Atlanta
+1 678.553.2100

Austin
+1 512.320.7200

Boca Raton
+1 561.955.7600

Boston
+1 617.310.6000

Chicago
+1 312.456.8400

Dallas
+1 214.665.3600

Delaware
+1 302.661.7000

Denver
+1 303.572.6500

Fort Lauderdale
+1 954.765.0500

Houston
+1 713.374.3500

Las Vegas
+1 702.792.3773

London*
+44 (0) 203 349 8700

Los Angeles
+1 310.586.7700

Mexico City+
+52 (1) 55 5029 0000

Miami
+1 305.579.0500

New Jersey
+1 973.360.7900

New York
+1 212.801.9200

Northern Virginia
+1 703.749.1300

Orange County
+1 949.732.6500

Orlando
+1 407.420.1000

Philadelphia
+1 215.988.7800

Phoenix
+1 602.445.8000

Sacramento
+1 916.442.1111

San Francisco
+1 415.655.1300

Seoul∞
+82 (0) 2 369 1000

Shanghai
+86 (21) 6391.6633

Silicon Valley
+1 650.328.8500

Tallahassee
+1 850.222.6891

Tampa
+1 813.318.5700

Tel Aviv^
+972 (0) 3 636 6000

Warsaw~
+48 22 690 6100

Washington, D.C.
+1 202.331.3100

Westchester County
+1 914.286.2900

West Palm Beach
+1 561.650.7900