# *A Standard for Securing Privacy in the Cloud*

*Using the ISO 27018 Standard*

---

*By Thomas M. Smith, CD, CISSP*

*December, 2017*

***ABSTRACT***

Privacy matters! With that in mind, securing personally identifiable information (PII) in the cloud environment can be a challenge for the cloud service provider as well as the cloud service customer. Each has unique privacy responsibilities as well as overlapping responsibilities.

There are legislative requirements that must be also met such as the requirements prescribed in the Canadian Personal Information Protection and Electronic Documents Act (PIPEDA). In the European Union there are ample provisions in the General Data Protection Regulation (GDPR) and elsewhere that have explicit privacy protection requirements.

This paper sets out the privacy related controls that are provided in the International Organization for Standardization (ISO) I 27018 *Code of practice for protection of personally identifiable in public clouds.* It identifies the controls that can be applied by a cloud service provider and provide assurances to its customers that it has reasonable privacy management practices in place.

information (PII) in public clouds. The controls in the Standard are intended to facilitate establishing adequate security in the protection of PII within a cloud environment. It is important to note that this Standard is predicated on the assumption that the service provider is using or intend to use the security controls as set out in ISO/IEC 27002 Standard. The application of the ISO 27018 Standard either enhances the existing controls or establishes additional controls that should be applied.

**Introduction**

While it has become common practice for organizations to merely develop or adopt a set of privacy principles to which they then espouse as adequate for their organization, this approach falls short of the legal and regulatory requirements. Merely displaying a set of principles or denying the collection and/or use of personal information is highly inappropriate. Organizations need to demonstrate that they have, in fact, applied adequate measures to ensure that the principles are not only adopted but also put into practice.

From a cloud environment perspective, this means that security controls must be established and appropriately implement to protect the PII from a service provider perspective. The cloud customer can and will expect to see how well the cloud service provider has established and implemented privacy practices to ensure that any PII will be adequately protected for or on behalf of a customer.

**Privacy Controls to be Implemented for the Cloud Environment**

The Standard provides the controls to facilitate adherence to basic privacy principles; however, it is generally designed to make additions or enhancements to security controls already established using the ISO 27002 Standard. The following outlines the various control categories and the controls that can be applied in these areas to protect PII within the service providers cloud facilities:

| *Control Category* | *Privacy Controls* |
|---|---|
| *Information Security Policies* | • *The information security policies should be updated to include indicators of senior management's support for and commitment to abiding by any applicable legal and regulatory requirements as well as those stipulated on contractual agreements respecting the protection of PII.* |
| *Human Resources Security* | • *Informa employees and others of the possible and likely consequences arising from a privacy or security incident or breach relating to both privacy and security of assets including PII.* |
| *Access Control* | • *Responsibilities for access management should be delineated and a service provider's architecture should take into account both the needs of the customer and the provider with capabilities that facilitate customers need to administer its own user* |

| | |
|---|---|
| | *accounts when necessary. This would include processes for customer's user registration/de-registration and password management when part of the service offering.* |
| *Cryptography* | • *The service provider should disclose its encrypting policies and where appropriate and without compromising its security, disclose the types of encryption be utilized. In addition, it may be necessary to coordinate/share certain security encryption services with the customer.* |
| *Operations Security* | • *Using PII for other than the intended purposes should be avoided, especially in the development and testing environments. In all cases, the service provider should assess the risks to PII outside of the production environment and ensure adequate mitigation measures are in place.*<br>• *Data backup policies should be disclosed to customers. In addition, off-site storage locations should also be known since PII could inevitably end up at n undesirable location for the customer and cause legal or regulatory non-compliance for the customer.*<br>• *Various logs should be agreement upon or made available to customers, especially to trach events relating to the customers' PII access and management needs.* |
| *Communications Security* | • *All media that contains PII and transferred into or out of the service provider facilities should be tracked. Where possible, cloud service customers should be encouraged to encrypt PII or employ other measures to ensure that the data can only be accessed at the point of destination and not while in transit.* |
| *Information Security Incident Management* | • *From a cloud environment perspective, there should be an expectation of shared responsibilities* |

| | |
|---|---|
| | *associate with privacy incidents. The cloud service provider may need to have the necessary procedures to ensure events affecting a customers' PII is known as well as allow the customer to track the status of the events when necessary.* |
| *Compliance* | • *The cloud service provider should be capable of demonstrating conformance to legal and regulatory requirements, its privacy principles as well as any customer specific contractual or other arrangements.* |

**Privacy Control Enhancements**

The ISO 27018 Standard also provides a number of enhancements to the controls around certain privacy principles:

| *ISO Privacy Principle* | *Control Enhancement(s)* |
|---|---|
| *Consent and choice* | *A.1.1 Obligation to co-operate regarding PII principals' rights* |
| *Purpose legitimacy and specification* | *A.2.1 Public cloud PII processor's purpose*<br>*A.2.2 Public cloud PII processor's commercial use* |
| *Collection limitation* | *Nil* |
| *Data minimization* | *A.4.1 Secure erasure of temporary files* |
| *Use, retention and disclosure limitation* | *A.5.1 PII disclosure notification*<br>*A.5.2 Recording of PII disclosures* |
| *Accuracy and quality* | *Nil* |
| *Openness, transparency and notice* | *A.7.1 Disclosure of sub-contracted PII processing* |
| *Individual participation and access* | *Nil* |
| *Accountability* | *A.9.1 Notification of a data breach involving PII*<br>*A.9.2 Retention period for administrative security policies and guidelines*<br>*A.9.3 PII return, transfer and disposal* |

| | |
|---|---|
| *Information security* | *A.10.1 Confidentiality or non-disclosure agreements* |
| | *A.10.2 Restriction of the creation of hardcopy material* |
| | *A.10.3 Control and logging of data restoration* |
| | *A.10.4 Protecting data on storage media leaving the premises* |
| | *A.10.5 Use of unencrypted portable storage media and devices* |
| | *A.10.6 Encryption of PII transmitted over public data-transmission networks* |
| | *A.10.7 Secure disposal of hardcopy materials* |
| | *A.10.8 Unique use of user IDs* |
| | *A.10.9 Records of authorized users* |
| | *A.10.10 User ID management* |
| | *A.10.11 Contract measures* |
| | *A.10.12 Sub-contracted PII processing* |
| | *A.10.13 Access to data on pre-used data storage space* |
| *Privacy compliance* | *A.11.1 Geographical location of PII* |
| | *A.11.2 Intended destination of PII* |

**Summary**

The division of responsibilities and the implementation of the additional controls are an excellent approach to resolving security controls management and expectations. Organizations would do well to document its own roles and responsibilities. A cloud service provider would be well served by also documented its roles and responsibilities as well as informing customers of their responsibilities.

From a cloud service provider perspective, implementing the controls as provided in the Standard can improve adoption of cloud services and mitigate legal and other issues that traditionally may arise between the parties involved in the service.

### *Bibliography*

*BSI, Extending ISO/IEC 27001 into the Cloud*

*European Union, General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679)*

*ISO, Information technology — Security techniques — Information security management systems — Requirements, ISO/IEC 27001*

*ISO Code of practice for protection of personally identifiable information, ISO/IEC 27018:2013,*

*ISO Information technology — Security techniques — Privacy framework, ISO IEC 29100*

*NIST, The NIST Definition of Cloud Computing, Special Publication 800-145*

*NIST, Guidelines on Security and Privacy in Public Cloud Computing, Special Publication 800-144*

*US Department of Commerce, Safe Harbor Privacy Principles, July 2000*