ISO/IEC 27018 Standard for Privacy on the Cloud – The Meaning for Public Bodies

March 4, 2015 - Chantal Bernier, LL.B., LL.M, Counsel, Dentons Canada LLP, former Interim Privacy Commissioner of Canada, Senior fellow, Graduate School of Public and International Affairs, University of Ottawa

Thanks to the foresight of Jennifer Stoddard, then Privacy Commissioner of Canada, the Office of the Privacy Commissioner of Canada (OPC) was a significant contributor to the drafting of ISO/IEC Standard 27018 – *A Code of Practice for PII protection in public clouds acting as PII processors*. The Standard was adopted on April 25, 2014. Microsoft announced on February 16, 2015 that it had received certification for compliance with the standard.

In my view, ISO/IEC Standard 27018 changes the landscape in relation to the cloud, particularly for public bodies, as it allows them to finally access the benefits of the cloud, and keep control of the data.

This conclusion applies to Saskatchewan as it does to other governments in Canada.

1. Saskatchewan OIPC on cloud computing

In its July 2010 issue of the FOIP Folio newsletter, the Saskatchewan Office of the Information and Privacy Commissioner (OIPC) describes cloud computing as the system through which the client accesses a shared pool of configurable computing resources on an on-demand basis through the Internet.

The OIPC summarises the benefits of the cloud in the same terms as the OPC: scalability, reliability, worldwide accessibility, cost savings, and efficiency.

The OIPC highlights privacy considerations around cloud computing contracts recommending "careful attention" to the following questions:

i) Will the data on the cloud still be under the control of the Saskatchewan organization for the purposes of FOIP, LA FOIP or HIPA?

ii) Will the data be adequately protected?

iii) Would the cloud computing impede the citizens right of access to information?

iv) How does the Saskatchewan organisation control secondary use or unauthorized access to its own data?

v) Is the 18 year old FOIP Act up to the task of addressing and overseeing cloud computing?

2. The answers of ISO/IEC Standard 27018

a) Data control over the cloud and secondary use

Under ISO/IEC 27018, the certified cloud provider must act only upon the instructions of the cloud customer:

> "Note that the cloud service customer has authority over the processing and use of the data. (…).the public cloud PII Processor having no data processing objectives other than those set by the cloud service customer with respect to the PII processes and the operations necessary to achieve the cloud service customer's objectives".

Specifically,

- A mechanism must be established by contract to ensure the cloud provider manages internal compliance with privacy protection laws of the cloud provider.
- The cloud provider must disclose to the cloud customer the geo-location in which the personal data may be stored.

b) Protection of the data

The ISO/IEC Standard 27018 offers greater protection than any Canadian privacy law, including Saskatchewan FOIP Act by requiring that,

- Contractual agreements clearly allocate responsibility between the cloud provider, its sub-contractors and the cloud service customer;
- The cloud provider promptly notify the cloud customer of a data breach as part of the contract;
- The cloud provider will reject any request from law enforcement for disclosure that is not legally binding; and even so, in consultation with the cloud customer,
- PII transmitted over public data transmission networks must be encrypted;
- Human resource security measures must be implemented. .

c) Access to information

The FOIP Act applies exclusively to "records that are in the possession or under the control of a government institution" (section 5). I am of the view that the entire direction of ISO/IEC Standard 27018 maintains the storage of the data on the cloud to the ongoing control of the cloud customer.

d) ISO/IEC Standard 27018 and the FOIP Act

The question raised in 2009-2010 as to the adequacy of the FOIP Act in relation to the cloud is answered, it seems to me, by the Standard, as it supplements domestic law with specific obligations of cloud providers.

.

Conclusion – The meaning of ISO/IEC Standard 27018 for public bodies

For public bodies in Canada, ISO Standard 27018 means more safety, same control.