Implementing Information Privacy Practices in Canada

Using the 830-03 CSA Privacy Model Code

By Thomas M. Smith, CD, CISSP

October, 2016

ABSTRACT

There are many reasons why an organization needs to establish and implement a good set of information privacy practices in Canada and elsewhere for that matter. There are legislative requirements that must be met such as the requirements prescribed in the Canadian Personal Information Protection and Electronic Documents Act (PIPEDA). In addition, Canadian organizations that conduct business outside of Canada, especially in the European Union and elsewhere are also expected to comply with privacy protection requirements.

This paper sets out a good set of privacy practices that will meet the basic requirements et out in PIPEDA while aiming to conform to the basic principles outlined in the CSA Code. They will also allow an organization to establish the basic privacy program framework around which other aspects of privacy can be adequately and efficiently managed.

Introduction

While it has become common practice for organizations to leave privacy and its management obligations to legal entities, it is becoming more important to involve other areas of the organization as well.

Information managers are key to the success of any privacy program and as such should be provided with specific guidance on best practices that can be applied in an efficient and effective manner.

A Canadian Model Code

The Canadian Standards Association (CSA) publishes an excellent model code (Q830-03) that can be adapted to any organization. The Q830 code was re-affirmed again in 2014 and can easily and quickly be adopted. The basic privacy principles espoused by CSA are:[1]

1. *Accountability: The organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.*
2. *Identifying Purposes: The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.*
3. *Consent: The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.*
4. *Limiting Collection: The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization; information shall be collected by fair and lawful means.*
5. *Limiting Use, Disclosure, and Retention: Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfilment of those purposes.*
6. *Accuracy: Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.*
7. *Safeguards: Personal information shall be protected by security controls appropriate to the sensitivity of the information.*

[1] CSA Model Code for the Protection of Personal Information, Q830-03.

8. *Openness: An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.*
9. *Individual Access: Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.*
10. *Challenging Compliance: An individual shall be able to address a challenge concerning compliance with these principles to a designated individual.*

Implementing Security Controls

To support these principles, there are several key practices that should be established and implemented such as:

- *Designating a point of contact and senior management person to be overall responsible for privacy compliance*
- *Communicate the title and contact information about the designated individual*
- *Identify all personal information holdings within the organization along with the business or other needs for the information*
- *Ensure that consent is obtained for the information*
- *State the reasons why it is necessary to have the personal information*
- *Ensure that the stated purposes are limited to what a reasonable person would expect under the circumstances*
- *Limit the amount and type of the information gathered to what is necessary for the identified purposes.*
- *Identify the kinds of personal information to be collected in in information policies and practices.*
- *Ensure that staff can explain why the information is needed when collecting or challenged about the personal information*
- *Document any new purpose for the use of personal information.*
- *Implement specific retention periods that take into account legal requirements and ensure mechanism are in place to update retained information as necessary*
- *Securely dispose of information that is no longer required*
- *Asses the impacts to privacy and the risks associated with unauthorized access use or disposal of sensitive personal information*

- *Include privacy awareness and practices during other briefings such as security briefings, along with regular reminders*
- *Establish helpful procedures that facilitate individual's request for information about the policy and practices as well as about their personal information*
- *Observe minimum response timings such as a 30-day limit which is generally acceptable with permissible exceptions*
- *Establish procedures to acknowledge and address complaints in professional and ethical manner.*
- *Provide simple and effective means to facilitate corrections, removal and or updates as needed*
- *Develop a sound privacy policy that supports basic requirements for implementing the principles and provides appropriate safeguards to protect the information*
- *Communicate privacy policies, practices, procedures and resolution mechanisms*

It is essential that any organization develop and implement the above basic practices or other similar controls in order to establish conformance with legal or regulatory requirements.

Summary

While these controls may appear burdensome or complex, they are not necessarily so but are evidence of an organizations fiduciary responsibilities for privacy.

Bibliography

Government of Canada, Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5

Canadian Standards Association, Model Code for the Protection of Personal Information, Q830-03 (re-affirmed 2014)

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

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

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

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