PIPEDA'S BREACH REPORTING REQUIREMENTS FINALIZED, TO COME INTO FORCE NOVEMBER 1, 2018

Posted on May 15, 2018

Categories: Insights, Publications

Through an Order in Council, the federal government has announced that certain sections of the Digital Privacy Act ("**DPA**") that amend the Personal Information Protection and Electronic Documents Act ("**PIPEDA**") will come into force on November 1, 2018. The Breach of Security Safeguards Regulations (the "**Regulations**") will also come into force on the same day.

The new notice obligation will require organizations to report a breach of security safeguards involving personal information where it is reasonable in the circumstances to believe that the breach creates a "real risk of significant harm"[1] to affected individuals. A "breach of security safeguards" is defined as a loss of, unauthorized access to or unauthorized disclosure of personal information resulting from a breach of an organization's security safeguards or from a failure to establish those safeguards.

This update provides an overview of the breach reporting requirements.

The Objectives of the Breach Reporting Obligations

The breach reporting obligations are designed to: (1) ensure that all Canadians receive the same information about data breaches that pose a risk of significant harm to them; (2) ensure that notifications of data breaches contain enough information to permit individuals to understand the significance and potential impact of the breach; (3) ensure that the Commissioner receives consistent and comparable information about breaches; and (4) ensure that the Commissioner can provide meaningful and effective oversight and verify that organizations are complying with their notification requirements.

Reporting to the Commissioner

The form and content of required notice is set out in the Regulations. Where an organization determines that a breach meets the requisite standard for notice, it will be required to deliver a written report to the Commissioner that, at a minimum, includes:

- a description of the circumstances of the breach and, if known, the cause;
- the day on which, or period during which, the breach occurred;

- a description of the personal information that is the subject of the breach;
- an estimate of the number of individuals in respect of whom the breach creates a real risk of significant harm;
- a description of the steps that the organization has taken to reduce the risk of harm to the affected individual resulting from the breach or to mitigate that harm;
- a description of the steps that the organization has taken or intends to take to notify each affected individual of the breach in accordance with PIPEDA; and
- the name and contact information of a person who can answer on behalf of the organization, the Commissioner's questions about the breach.

Notably, the Regulations do not require organizations to include an assessment of the potential harm likely to be caused, which is required when providing notice to the Information and Privacy Commissioner of Alberta under Alberta's Personal Information Protection Act.

Notifying Affected Individuals

Under the Regulations, where an organization determines that it is reasonable in the circumstances to believe that a breach involving personal information is likely to cause a "real risk of significant harm", it is required to deliver a notice to affected individuals that, at a minimum, includes:

- a description of the circumstances of the breach;
- the day on which, or period during which, the breach occurred;
- a description of the personal information that is the subject of the breach;
- a description of the steps that the organization has taken to reduce the risk of harm to the affected individual resulting from the breach or to mitigate that harm;
- a description of the steps that the individual could take to reduce the risk of harm resulting from the breach or to mitigate that harm;
- a toll-free number or email address that the affected individual can use to obtain further information about the breach; and
- information about the organization's internal complaint process and about the affected individual's right, under the PIPEDA to file a complaint with the Commissioner.

The Regulations require that notice be made directly to each individual via email, letter, telephone, or in person, unless: (1) the cost of doing so is prohibitive; (2) direct notification may cause further harm to the individual; or (3) the organization does not have contact information for the affected individual or the information it has is out of date. In such circumstances, the Regulations permit indirect notification through public announcements or advertising.

Notifying Other Organizations

Under the DPA, organizations may also be required to notify other organizations, a government institution or a part of a government institution of the breach, if the notifying organization believes that doing so may reduce the risk of harm that could result or mitigate that harm. The Regulations do not contain any requirements as to the content of notice to other organizations.

Record-Keeping

The Regulations impose record-keeping requirements on organizations with respect to any breach of security safeguards impacting personal information – whether or not a breach is likely to cause a real risk of significant harm to affected individuals.

Organizations must keep records of every breach of security safeguards for 24 months from the date the organization determines that the breach has occurred. The record of the breach must contain sufficient information to permit the Commissioner to verify whether the organization is complying with PIPEDA.

Impact

The amendments and detailed breach reporting obligations that are set out in the Regulations largely reflect previously articulated "best practices" established by the Office of the Privacy Commissioner for Ontario and existing statutory requirements in Alberta. Once in force, these requirements will bring Canada more closely in line with the General Data Protection Regulation – i.e., the European privacy requirements set to come into force on May 25, 2018. Equivalency in privacy protection allows for the free flow of personal information from EU to Canadian organizations.

In light of these new legal requirements, organizations should ensure that:

1. all staff are trained to recognize and report any actual or potential data breach;
2. they have developed and tested their breach response plan; and
3. they maintains records of each data breach involving personal information under their control.

One of the objectives of the notice requirements is to allow the Commissioner to provide better oversight. Accordingly, data breach records will be compellable by the Commissioner to verify compliance.

Knowingly failing to report to the Commissioner, notify affected individuals, or maintain records could attract a fine of up to $100,000.

The determination of whether it is reasonable in the circumstances to believe that a breach involving personal information is likely to cause a "real risk of significant harm" is not always straightforward. Organizations that

experience a breach of their security safeguards are encouraged to contact privacy professionals immediately to determine whether a particular breach requires notification and to avoid incurring significant penalties for non-compliance.

by Lyndsay Wasser and Mitch Koczerginski

[1] Defined to include “bodily harm, humiliation, damage to reputation or relationships, loss of employment or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property.”

A Cautionary Note

The foregoing provides only an overview and does not constitute legal advice. Readers are cautioned against making any decisions based on this material alone. Rather, specific legal advice should be obtained.