
# SNEAK PEEK AT PIPEDA'S BREACH REPORTING REQUIREMENTS - PROPOSED REGULATIONS RELEASED FOR COMMENT

*Posted on September 8, 2017*

**Categories:** Insights, Publications

In June 2015, the Digital Privacy Act ("**DPA**") amended the Personal Information Protection and Electronic Documents Act ("**PIPEDA**")[1]. Once in force, organizations will be required to report data security incidents involving personal information where it is reasonable in the circumstances to believe that the breach creates a "real risk of significant harm"[2] to affected individuals. Under these new provisions, notice is required to be made to the Privacy Commissioner of Canada (the "**Commissioner**"), affected individuals and other organizations.

This update provides an overview of the recently proposed regulations which detail the content and method of the required notice. Our original bulletin on the DPA can be viewed here.

**The Objectives of the Proposed Regulations**

The proposed regulations 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.

The proposed regulations seek to satisfy the above-noted objectives by requiring that organizations carefully assess data breaches that occur and notify regulators, individuals and third party organizations as appropriate. Under the proposed regulations, an organization that experiences a data breach is required to determine 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" by conducting a risk assessment. If the organization determines that this threshold is met, it must:

1. Report the breach to the Commissioner as soon as feasible;
2. Notify affected individuals as soon as feasible;
3. Notify any other organization that might be able to mitigate the harm; and

4. Maintain a record of the data breach for 24 months and provide it to the Commissioner upon request.

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

**Reporting to the Commissioner**

Under the proposed 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 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 the Commissioner's questions about the breach on behalf of the organization.

Notably, organizations are not required to include an assessment of harm likely to be caused, which is required when providing notice to the Alberta Commissioner under Alberta's *Personal Information Protection Act*.[3]

**Notifying Affected Individuals**

Under the proposed 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 PIPEDA to file a complaint with the Commissioner.

The proposed 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 would 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 proposed regulations do not contain any requirements as to the content of notice to other organizations.

**Record-Keeping**

The proposed regulations impose record-keeping requirements on organizations with respect to any breach of security safeguards – whether or not the organization has determined 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".

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 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 *EU General Data Protection Regulation*, the European privacy requirements set to come into force in 2018. Equivalency in privacy protection allows for the free flow of personal information from EU to Canadian organizations.

Upon implementation, organizations should take care to maintain records of each data breach involving

personal information under its control. One of the objectives of the regulations is to allow the Commissioner to provide better oversight. Accordingly, data breach records will be compellable by the Commissioner to verify compliance.

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 straight forward. 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 Mitch Koczerginski, Kelly Kan, Articling Student

[1] *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5.[ps2id id='1' target=''/]
[2] 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."[ps2id id='2' target=''/]
[3] *Personal Information Protection Act*, SA 2003, c P-6.5.[ps2id id='3' target=''/]

**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.