AMSBIZLAW

ANALYSIS • OPINION • INSIGHT

ALLEN McDONALD SWARTZ LLP
Business Lawyers

MANDATORY DATA BREACH REPORTING REQUIREMENTS TAKE EFFECT ON NOVEMBER 1, 2018

IS YOUR ORGANIZATION READY?

"An organization that knowingly fails to (i) report a data breach to the OPC, (ii) notify affected individuals, or (iii) maintain records of a breach will be guilty of an offence punishable by fines of up to a maximum of Cdn$100,000 per occurrence."

By Jillian Swartz
October 16, 2018

On November 1, 2018, new mandatory notice requirements and new record-keeping requirements will come into force for organizations regulated by the federal Personal Information Protection and Electronic Documents Act ("PIPEDA").

When does the Obligation to Report and Notify arise?

Under the new requirements, if an organization experiences a breach of security safeguards involving personal information under its control and if it is reasonable to believe that the breach poses a "real risk of significant harm", that organization is required to:

1. report the breach to the Office of the Privacy Commissioner of Canada (the "OPC");

2. notify the affected individuals; and

3. in certain circumstances, notify other organizations.

PIPEDA defines "significant harm" quite broadly to include bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property. The term "real risk of significant harm" is not defined; however, PIPEDA does point to some factors that must be considered in making an assessment of whether this threshold has been met, namely the sensitivity of the personal information involved in the breach, the probability that the personal information has been, is, and/or will be, misused and other factors that are included in future regulations. The OPC has issued draft guidance and a draft reporting form that will assist organizations to understand and satisfy their new obligations; the deadline for feedback was October 2, 2018, so final guidance should be available shortly.

What are the Notification Requirements?

Notice to the OPC

A breach of security safeguards is the loss of, unauthorized access to, or unauthorized disclosure of personal information resulting from either a breach of an organization's security safeguards or a failure to establish those safeguards. Where a breach involves personal information under the organization's control and it is reasonable to believe that the breach creates a "real risk of significant harm" to an individual, that organization must report the breach the OPC as soon as feasible after the organization determines that the breach has occurred. The regulations prescribe the content, form and manner of reporting, which requires the following information to be included in the notice:

- the circumstances of the breach and the cause of the breach, if known
- the timeframe during which the breach occurred
- the type(s) of personal information that were accessed as a result of the breach, to the extent known
- the number (or approximate number) of individuals affected by the breach
- a description of the steps that the organization has taken to reduce the risk of harm that could result from the breach
- the steps that the organization has taken or intends to take to notify affected individuals
- the name and contact information of a person who can answer, on behalf of the organization, the OPC's questions about the breach

In addition, the regulations contemplate that an organization may not have complete information at the time a report is made, and specifically allow an organization to submit new information to the OPC after the initial report has been submitted.

Notice to Affected Individuals

The new regulations also require that notice be provided to affected individuals as soon as feasible after the organization confirms that the breach has occurred. Once

again, the regulations prescribe the content, form and manner of notification are prescribed by the regulations, including:

- a description of the circumstances of the breach
- the timeframe during which the breach occurred
- a description of personal information that is the subject of the breach, to the extent known
- a description of the steps that the organization has taken to reduce the risk of harm that could result from the breach
- a description of the steps that affected individuals could take to reduce the risk of harm
- contact information that the affected individual can use to obtain further information about the breach

What are the Record-Keeping Requirements?

PIPEDA requires organizations to keep and maintain records of all data breaches, including those that do not meet the "real risk of significant harm" threshold that triggers the reporting and notification obligations described above. Records of all data breaches must be maintained for 24 months from the day that the organization determined that the breach occurred. Moreover, these records must be provided to the OPC upon request, and must contain sufficient information to enable the OPC to verify compliance with the mandatory breach reporting provisions of PIPEDA. Based on the draft guidance issued by the OPC, the record should contain at least the following information:

- the date or estimated date of the breach
- a general description of the circumstances of the breach
- a description of the nature of information involved in the breach
- whether or not the breach was reported to the OPC
- whether or not affected individuals were notified
- if the breach was not reported to the OPC or the affected individuals were not notified, a brief explanation of why the breach was determined not to pose a "real risk of significant harm"

The record-keeping requirement is perhaps one of the most challenging aspects of PIPEDA's new obligations as it will require organizations to implement policies and procedures to ensure that all breaches (regardless of their significance) are recorded in a central database. These policies and procedures will need to be sufficient to prove to the OPC that your organization has complied with the new rules.

What are the potential penalties?

An organization that knowingly (i) fails to report a data breach to the OPC, (ii) notify affected individuals, or (iii) maintain or keep records of a breach will be guilty of an offence punishable by fines of up to a maximum of Cdn$100,000 per occurrence. Organizations should take note that where the failure relates to notifying affected individuals, it is a separate offence for every individual left without notification of the data breach, so the fines can add up very quickly.

Conclusion

One final note – this is a good time to update your organization's privacy policy or to create a privacy policy if your organization does not already have one. It is critical that data breach plans be tested regularly (and ideally before the new rules come into effect), so that your organization is ready for the "when" not "if" a data breach occurs. Finally, you may also wish to consider obtaining cyber insurance to cover, among other things, the costs of the notification process.

The lawyers at Allen McDonald Swartz LLP have significant experience advising on privacy maters. If your organization needs more information about the impact of the new regulations or assistance drafting or updating your privacy policy, please contact Jillian Swartz by phone at 416.262.8206 or by email at jswartz@amsbizlaw.com or any member of the AMS team.