

# PIPEDA – Draft Breach of Security Safeguards Regulations Published

Anti-Spam | Business Law | Corporate & Commercial | Corporate Law | Privacy Law | Technology

25 September 2017

The *Digital Privacy Act*, passed in June 2015, made a number of amendments to Canada's federal private sector privacy law, the *Personal Information Protection and Electronic Documents Act* ("PIPEDA"). Key among these amendments was the establishment of mandatory data breach reporting and notification obligations, as well as record-keeping obligations, although these provisions were not proclaimed in force pending the finalization of related regulations.

On September 2, 2017, draft Breach of Security Safeguards Regulations were published for a 30 day comment period.

The draft Regulations provide further details pertaining to an organization's obligations for reporting a data breach – referred to as a "breach of security safeguards" – to the Privacy Commissioner of Canada (the "Commissioner") and for notifying affected individuals, the manner of notification, and record-keeping requirements.

A "breach of security safeguards" is defined under PIPEDA as a loss of, unauthorized access to or unauthorized disclosure of personal information resulting from either the breach of an organization's security safeguards or a failure to establish those safeguards.

Once in force, the data breach provisions of PIPEDA and the Regulations will require an organization to report to the Commissioner any breach of security safeguards involving personal information under its control if it is reasonable in the circumstances to believe that the breach creates a "real risk of significant harm" to an individual. The organization will also be required to notify any affected individuals and any other organization or government institution that may be able to mitigate the harm to affected individuals. The report and notification must be made as soon as feasible after the organization determines that a breach has occurred.

"Significant harm" includes 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. Factors organizations must consider in assessing whether a breach creates a "real risk of significant harm" to an individual include the sensitivity of the personal information involved and the probability that the personal information has been, is being, or will be misused.

## **Content, Form and Manner of Report to Commissioner**

Pursuant to the draft Regulations, a report to the Commissioner must be in writing and contain, at a minimum:

- a description of the circumstances of the breach and, if known, the cause;
- the day on which, or the 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 for whom the breach creates a real risk of significant harm;
- a description of the steps that the organization has taken to reduce or mitigate the risk of harm to each affected individual resulting from the breach;
- a description of the steps that the organization has taken or intends to take to notify each affected individual of the breach; and
- the name and contact information of a person who can answer, on behalf of the organization, the Commissioner's questions about the breach.

## **Content and Manner of Notification to Affected Individuals**

Notification to an affected individual must contain sufficient information to allow the individual to understand the significance to them of the breach and to take steps, if possible, to reduce or mitigate the risk of harm that could result. Pursuant to the draft Regulations, a notification to an affected individual must contain,

at a minimum:

- 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 or mitigate the risk of harm to the individual resulting from the breach;
- a description of the steps that the individual could take to reduce or mitigate the risk of harm resulting from the breach;
- a toll-free number or email address that the individual can use to obtain further information about the breach; and
- information about the organization's internal complaint process and the individual's right, under PIPEDA, to file a complaint with the Commissioner.

Except in limited circumstances, notification must be given directly to an affected individual and may be given by email or other secure form of communication (if the individual has consented to receiving information in that manner), letter, telephone or in person. Indirect notification, by means of a conspicuous message posted on the organization's website or an advertisement, is to be given if direct notification would cause further harm to the affected individual, the cost of direct notification is prohibitive, or the organization does not have current contact information for the affected individual.

### Record-Keeping Requirements

Once in force, the data breach provisions of PIPEDA and the Regulations will require organizations to maintain a record of every breach of security safeguards for a minimum of 24 months after the day on which the organization determines that the breach has occurred, and provide it to the Commissioner upon request. The record must contain sufficient information to enable the Commissioner to verify compliance with the data breach reporting and notification requirements above.

### Coming into Force

Interested persons may submit comments concerning the draft Regulations until October 2, 2017. Once the Regulations are final, they will come into effect at the same time as the related statutory requirements under PIPEDA. The Government has indicated that there will be a delaying coming into force after publication to allow organizations to prepare. In the interim, organizations should consider reviewing and, if necessary, adjusting their breach reporting, notification and record-keeping procedures in light of the anticipated requirements.

*(This blog is provided for educational purposes only, and does not necessarily reflect the views of Gardiner Roberts LLP).*

## Author



**Catherine Carscallen**

Partner

416.865.6654

ccarscallen@grllp.com



**Bay Adelaide Centre — East Tower**  
22 Adelaide Street West, Suite 3600  
Toronto, ON M5H 4E3

Phone: 416.865.6600  
Fax: 416.865.6636  
contactGR@grllp.com