COMPLIANCE BULLETIN

HIGHLIGHTS

- Starting Nov. 1, 2018, Canada's federal Personal Information Protection and Electronic Documents Act (PIPEDA) will require organizations that suffer a data breach involving personal information to:
  - Report the breach to the Privacy Commissioner of Canada.
  - Give notice of the breach to affected individuals.
  - Maintain records of data breaches that affect personal information.
- In order to avoid fines and penalties, organizations will need to understand the basic requirements of PIPEDA.

Federal Data Breach Regulations Take Effect Nov. 1, 2018

OVERVIEW

Starting Nov. 1, 2018, Canada's federal Personal Information Protection and Electronic Documents Act (PIPEDA) will require organizations that suffer a data breach involving personal information to:

1. Report the breach to the Privacy Commissioner of Canada (Commissioner).
2. Give notice of the breach to affected individuals.
3. Maintain records of data breaches that affect personal information.

In order to avoid fines and penalties, organizations will need to understand PIPEDA and its basic requirements.

BACKGROUND

PIPEDA is Canada's federal privacy law that governs the collection, use and disclosure of personal information in the course of commercial activities by private sector organizations and federally regulated businesses. In 2015, PIPEDA was amended by the Digital Privacy Act (DPA), an act that made a number of important changes to PIPEDA.

While most of the amendments contained in the DPA came into force in 2015, the mandatory data breach notification, reporting and record-keeping provisions weren't initially enforced. Instead, the law

Megson FitzPatrick INSURANCE SERVICES

indicated that they would be brought into force only after corresponding regulations were finalized.

On Sept. 1, 2017, the Canadian government published draft regulations relating to these requirements. The government accepted public comments on the draft regulations until Oct. 2, 2017, after which time the government completed its consultation process. The government recently published and announced that mandatory breach notifications under the PIPEDA will be enforced beginning Nov. 1, 2018.

The amended PIPEDA applies to organizations' commercial activities across all provinces, except in provinces where equivalent privacy laws exist. To date, Alberta, British Columbia and Quebec have implemented laws deemed to be substantially similar to PIPEDA. Moreover, New Brunswick, Newfoundland and Labrador, Nova Scotia and Ontario are partially exempt from PIPEDA, as these provinces have adopted similar legislation with respect to personal health information.

OVERVIEW OF THE REGULATIONS

There are effectively three major sections of PIPEDA to be aware of—reports to the Commissioner, notifications to affected individuals and record-keeping. The following is an overview of the requirements that employers need to consider:

Reports to the Commissioner

If an organization suffers a breach of security safeguards involving personal information under its control and it is reasonable to believe that the breach creates a real risk of significant harm to an individual, then the organization must report the breach to the Commissioner after the organization determines that the breach has occurred. According to the regulation, a report to the Commissioner must be made in writing and contain the following information:

- 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 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 each 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.
- The name and contact information of a person who can answer, on behalf of the organization, the Commissioner’s questions about the breach.

Under the regulations, data breach reports can be submitted with the best information available to the organization at the time. This allows organizations to report breaches quickly and take the appropriate actions, even when key information regarding the incident is not yet available.

Communications to the Commissioner should be made via a secure means. Companies are encouraged to refer to the key steps in responding to a privacy breach released by the Commissioner. These steps, as well as supplementary information on responding to breaches, can be found here.

Requirements for Notifying Affected Individuals of a Data Breach

If an organization suffers a breach of security safeguards involving an individual's personal information under the organization's control and it is reasonable to believe that the breach creates a real risk of significant harm to the individual, then the organization must notify the individual of the breach. Notifications must be given as soon as possible after the organization determines a breach has occurred.

Notification to an affected individual must contain sufficient information to allow the individual to:

1. Understand the significance of the breach.
2. Take any available steps to reduce the impact of the breach.

Per the regulations, a notification to an affected individual must contain the following:

- A description of the circumstances of the breach.
- The day or time frame the breach occurred.
- Descriptions of the type of personal information that was compromised during 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 affected 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 impacted individuals can use to obtain further information regarding the breach.

Notifications must be given directly to impacted individuals through an email, letter (delivered to the last known home address of the affected individual), telephone call, in-person conversation or other secure form of communication if the affected individual consented to receiving information from the organization in that manner. Under limited circumstances, organizations will be allowed to provide affected individuals with indirect notification of a data breach. According to the regulations, organizations will be able to provide indirect notification only if:

- A direct notification would cause further harm to the affected individual.
- The cost of giving a direct notification is prohibitive for the organization.
- The organization does not have contact information for the affected individual or the information that it has is out of date.

The regulations indicate that indirect notification may be given only by either a conspicuous message, posted on the organization's website for at least 90 days, or by means of an advertisement that is likely to reach the affected individuals.

Record-keeping Requirements

PIPEDA requires organizations to maintain a record of every breach of security safeguards. The regulations state that organizations must maintain these records for a minimum of 24 months after the day on which the organization determines that the breach has occurred, and provide them 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.

An important distinction here is that records must be maintained for every data breach, and not just those that create a real risk of significant harm. This means that organizations will be required to keep records of data breaches even if they don't have to report the breach to the Commissioner or notify affected individuals.

NEXT STEPS

Organizations should take the proper steps to ensure they are PIPEDA compliant. While the new reporting and record-keeping requirements appear to place an administrative burden on organizations, companies that already have cyber security protocols in place will likely experience minimal impact. Some general preparations to consider include the following:

1. Ensure you are informed on all the new requirements.
2. Prepare for data breach scenarios.
3. Train your employees.
4. Update your internal processes.
5. Assess your data storage and response strategies.
6. Obtain the proper insurance coverage.

To learn more about the regulations, you can read a detailed impact analysis statement and the regulation's text through the Canada Gazette. Megson FitzPatrick Insurance Services will continue to monitor legislative changes and provide updates as necessary.