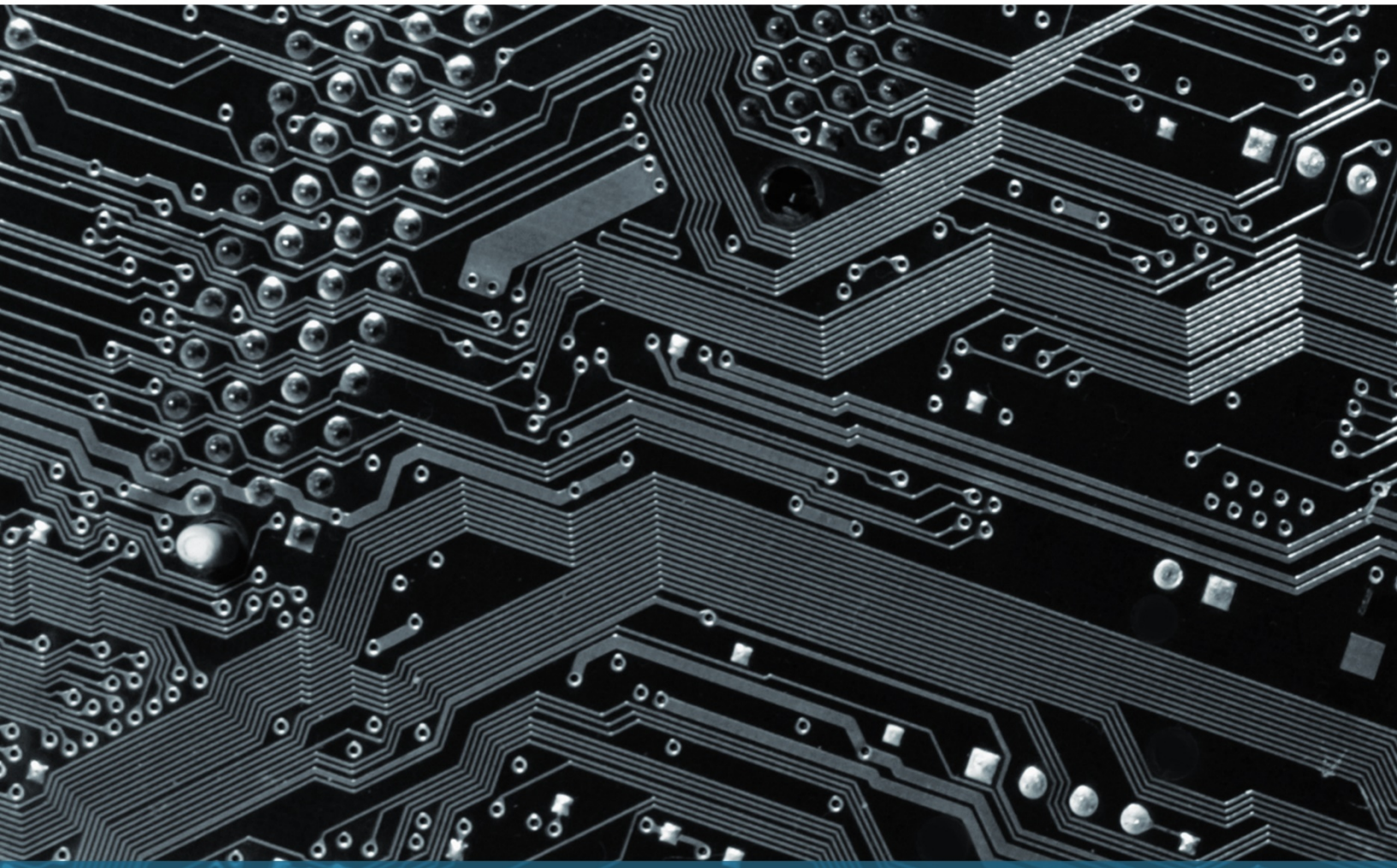

Digital Privacy Act:
Canada's Data Breach Notification Rules

PROVIDED BY

Megson FitzPatrick Insurance Services

(250) 595-5212

www.megsonfitzpatrick.com

Megson FitzPatrick
INSURANCE SERVICES

TABLE OF CONTENTS

INTRODUCTION

With each passing year, malicious cyber events increase in size and severity, impacting companies and customers alike. Small and medium-sized businesses are common victims of hackers, as their security measures tend to be easier to crack. However, even global organizations like Yahoo, eBay and Target that have invested substantial sums into cyber security programs are not immune from the threat of a data breach.

> In 2016 alone, more than 1.3 billion records were lost or stolen worldwide, with North America accounting for 80 per cent of known incidents, according to a report from PricewaterhouseCoopers Canada.

Canada itself has seen an increase in cyber security incidents, with the number of businesses reporting a loss or exposure of sensitive data over a 12-month period increasing every year for the past three years and 8 per cent overall.

When data breaches occur, they can result in a major financial and reputational hit for a company. These costs are rising for businesses, with estimates suggesting that data breaches will cost the global economy over $2 trillion between 2014 and 2019. What's more, when sensitive data (e.g., credit card numbers and personal identifiable information) is involved, a company's clients and customers can also experience stressful and damaging losses.

With no clear end to an ever-shifting, dangerous cyber landscape and with confidential information on the line, the federal government recently re-evaluated organizational requirements and oversight related to data breaches. This re-evaluation came through the enactment of the Digital Privacy Act (DPA), which amends the Personal Information Protection and Electronic Documents Act (PIPEDA).

BACKGROUND ON THE DPA AND PIPEDA

PIPEDA, as amended by the DPA, changes the way Canadian businesses handle data breaches. In order to understand the new rules and obligations, it's important to have a basic understanding of PIPEDA and the DPA.

When it comes to digital oversight, the Office of the Privacy Commissioner of Canada (Commissioner) is responsible for protecting and promoting privacy rights of Canadians. Among other duties, this body ensures that organizations comply with PIPEDA, a federal privacy law that received royal assent April 13, 2000.

PIPEDA establishes rules for how businesses handle personal information in commercial settings. Under PIPEDA, individuals must give consent for their personal information to be collected by businesses. The law requires businesses to limit the information they collect and put appropriate data security safeguards in place.

With the enactment of PIPEDA, both the cyber landscape and the ways of doing business in Canada changed. As the rate of data breaches increased, the federal government took note and looked to strengthen its regulatory framework for protecting personal information. To this end, the federal government introduced the DPA, which received royal assent June 18, 2015.

Simply put, the DPA amends PIPEDA and creates three new requirements that force businesses to rethink their data security practices. The DPA requires organizations to maintain records of all data breaches, report most data breaches to the Commissioner and disclose harmful data breaches to affected individuals.

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, these requirements came into force Nov. 1, 2018. The final text of the regulations—which outlines what's required in a company's report to the Office of the Privacy Commissioner (OPC) and affected individuals following a data breach—can be found here. To comply with the new requirements, organizations must update breach response protocols, establish legal frameworks, create a breach response team, design templates for data breach reports, create a system for retaining data breach records, and update internal policies and training materials.

To help organizations better understand their obligations, the OPC recently published final guidance on the law. Additionally, businesses should maintain a strong grasp of the DPA and how the new regulations affect the way they respond to data breaches.

APPLICABILITY

The amended PIPEDA applies to organizations' commercial activities in all provinces, except in provinces that have equivalent privacy laws. 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.

It should be noted that, even in provinces with equivalent privacy laws, PIPEDA applies to federally regulated employers and interprovincial commercial activity involving personal information.

OVERVIEW OF NEW REQUIREMENTS

The requirements set forth in PIPEDA, as amended by the DPA, are designed to keep Canadians informed anytime a data breach poses a threat to their personal information. The DPA amendments attempt to accomplish this goal by requiring organizations to do the following:

1. **Submit a written report to the Commissioner** anytime a data breach causes a real risk of significant harm to personal information under the organization's control.

2. **Notify individuals** anytime there is a data breach that affects the individual's information and creates a real risk of significant harm to the individual.

3. **Keep and maintain records** of every data breach involving personal information under the organization's control.

The following sections will take a detailed look at the three new requirements created by the DPA.

Reports to the Commissioner

Reporting data breaches to the Commissioner is a major aspect of PIPEDA, and there are specific rules related to the content, form and manner of these reports.

According to PIPEDA, an organization must 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. These reports will need to be submitted to the Commissioner as soon as possible after the data breach is discovered by the organization. When it comes to submitted reports to the Commissioner, there are several concepts to consider:

- **Breach of security safeguards**—PIPEDA broadly defines a breach of security safeguards as "the loss of, unauthorized access to or disclosure of personal information resulting from a breach of an organization's security safeguards or from a failure to establish those safeguards." Per the OPC guidance, security safeguards include physical, organizational and technological measures designed to protect against the loss, theft and unauthorized access, disclosure, copying, use or modification of personal information.
- **Personal information under the control of an organization**—Under PIPEDA, the obligation to report a hack rests with the organization that controls the personal information implicated in the breach itself. PIPEDA does not explicitly define what it means by "control." However, PIPEDA's accountability principle states that an organization remains responsible for personal information even if it has transferred it to a third party for processing. As such, in the event that a third party is breached, the organization originally in control of the information would have to

submit a report to the OPC and affected individuals. As a result, organizations need to ensure their third-party contracts address PIPEDA compliance and state who is responsible for reporting a breach should one occur.

- **Significant harm**—Not every breach needs to be reported to the OPC—just the ones that create a real risk of significant harm. The guidance from the OPC clarifies significant harm to include bodily harm, humiliation, damage to reputations or relationships, loss of employment, loss of business or professional opportunities, financial loss, identity theft, negative effects on credit records, and damage to or loss of property. In its guidance, the OPC noted that, even if just one record is compromised in a breach, it must still be reported if significant harm exists. When determining whether a breach of security safeguards creates a real risk of significant harm, organizations must consider the sensitivity of the personal information involved and the probability that the personal information has been, is or will be misused. Failure to report a breach could result in a fine as high as $100,000.

In determining whether a data breach creates a real risk of significant harm, PIPEDA instructs organizations to consider the following:

- The sensitivity of the personal information involved in the breach
- The probability that the personal information has been, is being or will be misused
- Other factors that the government might prescribe in the future

In its guidance, the OPC provides a model form organizations are encouraged to use to report a breach. The OPC also clarified that information can be added to reports that have already been submitted. Organizations must submit these reports as soon as feasible.

Content of Reports to the Commissioner

Reports to the Commissioner will need to 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 compromised in the breach
- An estimate of the number of individuals impacted by the breach
- A description of the steps that the organization has taken to reduce the risk of harm to each affected individual
- A description of the steps that the organization has taken or intends to take to notify each affected individual
- The name and contact information of a person who can answer, on behalf of the organization, the Commissioner's questions about the breach

What's more, data breach reports will only need to 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. If an organization becomes aware of any new information following an initial report to the Commissioner, they should submit any new details as soon as possible. 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.

Notification to Affected Individuals

In addition to making reports to the Commissioner, PIPEDA will also require organizations to notify individuals affected by a data breach. Notifications are similar to the reports given to the Commissioner.

According to the amended PIPEDA, unless otherwise prohibited by law, an organization must notify an individual of any breach of security safeguards involving the individual's personal information, particularly if the breach creates a real risk of significant harm to the individual.

Content of Notifications

Notifications to affected individuals must contain sufficient information to allow the individual to understand the significance of the breach and to take any available steps to reduce the impact of the breach.

Notifications must be provided to affected individuals as soon as feasible after a data breach is discovered and contain the following information:

- 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 was affected by 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 that the affected individual can use to obtain further information about the breach

Manner of Notification

In most cases, organizations will be required to directly notify an affected individual of a data breach. Direct notifications to individuals must be given in one of the following ways:

- By email or any other secure form of communication if the affected individual has consented to receiving information from the organization
- By letter delivered to the last known home address of the affected individual
- By telephone
- By in-person notification

Under limited circumstances, businesses will be allowed to provide affected individuals with indirect notification of a data breach. Organizations will be able to provide indirect notification only if any of the following is true:

- 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

Indirect notification may be given by either a highly visible message (posted on the organization's website for at least 90 days), or through the use of an advertisement that is likely to reach the affected individuals.

Data Breach Record-keeping

The data breach provisions of the amended PIPEDA require organizations to maintain a record of **every** data breach. Organizations must maintain these records for at least 24 months after the day the breach occurred and provide them to the Commissioner upon request.

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.

Records must contain sufficient information to enable the Commissioner to verify compliance with the data breach reporting and notification requirements above. It should be noted that a breach report to the Commissioner may be used by the organization as a record of the breach.

Requiring data breach records will provide a much-needed source of information on data security incidents in Canada, which could lead to a shared understanding of cyber security threats. Additionally, data breach records will provide key metrics, which will allow the government to create evidence-based policies regarding cyber security.

THE IMPACT ON BUSINESSES

Up until now, many Canadian organizations have not had to deal with the administrative burden of complying with data breach laws. As such, the introduction of the mandatory privacy breach notifications, reporting and record-keeping requirements found in the DPA have a sweeping impact on commercial businesses. In fact, the rules present new costs, risks and challenges for organizations, particularly as they relate to legal risk management, compliance and incident response planning.

Unless your organization already employs data security practices, the cost of protecting your business from a breach and any subsequent fines and litigation costs can be steep. Initially, businesses may incur expenses when taking the following steps to bolster their data security infrastructure:

- Creating policies and procedures
- Hiring legal professionals in the event of a breach
- Purchasing and implementing technology to help prevent a cyber event
- Hiring IT security professionals
- Training employees

However, these costs pale in comparison to the financial impact of a breach itself. In Canada, just one large-scale, cyber security incident can cost organizations upward of $5 million when you consider expenses like forensics, auditing, consulting and lost business. Ultimately, those that embrace cyber security best practices are much less vulnerable to cyber threats and the PIPEDA compliance burden that follows. Data security and due diligence are especially important when you consider the cost of non-compliance.

Moreover, fines for violating the data breach reporting requirements under PIPEDA range from $10,000 to $100,000 per occurrence. These fines do not include the cost of defending claims, which can be even more expensive and can come from a variety of sources.

Most experts believe that data breach disclosures will lead to increased business-to-business and consumer-to-business litigation. Not only do legal fees for these types of litigation often reach six figures, they are on the rise in Canada. In fact, according to the report, Cyber Security in Canada: Trends and Legal Risks, the country litigation activity, class-action certifications, and damage awards for privacy and information security incidents have steadily increased year over year since 2013.

Outside the internal, compliance and legal costs of complying with PIPEDA, organizations impacted by a breach could also face serious reputational harm. As part of the DPA amendments, organizations will have to make severe data breaches public when they notify affected individuals. This not only paints companies poorly in the public eye, but it can also have a lasting effect on an organization's bottom line.

A strong reputation has the potential to be your largest asset, but just one data breach could irreversibly tarnish your image, destroy any trust you've built through years of service and drive customers away.

Together, the costs of preparing for PIPEDA, defending your organization in court and dealing with reputational damages can be overwhelming for even the most profitable businesses. As such, it's critical that companies are diligent and thorough when preparing for PIPEDA.

6 WAYS TO RESPOND TO PIPEDA

Organizations that fail to properly respond to PIPEDA will likely struggle when faced with the new data breach requirements. Given the reach of the new rules, it's important that organizations do the following:

Ensure you are informed on all the new requirements. While this document provides a general overview of the requirements, it is not meant as a compliance guide. Organizations must review the final regulations and set aside time to understand their impact.

Prepare for data breach scenarios. No organization wants to be impacted by a data breach. One of the best ways to avoid a costly cyber incident and the administrative stress of the notification and reporting requirements of the DPA amendments is to mitigate the risk of a cyber attack altogether. The following are common scenarios that could lead to a data breach:

a. A laptop or storage device goes missing
b. A document that includes customers' or employees' personal information is mailed incorrectly
c. Personal information is accidentally posted or disposed of in an area that is accessible by the public
d. A network is compromised due to hacking or a security failure
e. Physical documents are lost or stolen
f. Backup data is lost
g. Customer or employee information is lost by a third-party vendor
h. Employee negligence or fraud occurs

Train your employees. When it comes to data breaches, employees are often a company's biggest exposure. In fact, according to the Ponemon Institute, 28 per cent of data breaches in 2017 were due to human error among employees or contractors. As such, organizations should ensure their employees have a deep understanding of data breaches—particularly how they occur and how to prevent them.

Ensure your internal processes are up to date. Staying organized and having clear procedures in place can go a long way in preventing a data breach. Review and update your existing protocols and policies to account for detecting, responding and reporting data breach incidents internally.

Assess your data storage practices and response strategies. Evaluate the types of information—personal information, intellectual property, supplier data, etc.—you hold and how you would respond in the event of a breach. Create a data breach incident response plan if one does not already exist. Such a plan should include methods for notifying the Commissioner and any impacted individuals.

Obtain the proper insurance coverage. Ensure that you have sufficient insurance in place and have taken the steps to mitigate any litigation exposures. Such steps can include requiring employee training, performing security audits and identifying cyber security vendors.

Without considering the above strategies, companies will no doubt be unprepared for the onslaught of legal risk management, compliance and incident response planning exposures created by the DPA and PIPEDA.

CONTACT YOUR BROKER TODAY

Cyber exposures are vast and not going anywhere anytime soon. Proper cyber liability insurance is essential to managing your company's risk and having the resources needed to meet the demands of PIPEDA.

The level of cyber coverage your business needs is based on your individual operations and can vary depending on your range of exposure. That's why it is important to work with a broker who can identify your areas of risk so a policy can be tailored to fit your situation. Contact Megson FitzPatrick Insurance Services today for more information on cyber insurance and useful risk management strategies.