YOCTO | LAW
PROFESSIONAL CORPORATION

October 19, 2018

New PIPEDA Data Breach Reporting and Notification Requirements: What You Need to Know Know

The *Personal Information Protection and Electronic Documents Act* ("**PIPEDA**" or the "**Act**") provides the privacy legislation framework for Canadian organizations that operate in the private sector.

PIPEDA requires organizations to protect information that they collect about an identifiable individual. This information is defined as "personal information" under the Act. Personal information includes personal e-mail addresses, home address, personal telephone number, age, date of birth, health or social insurance number, income, marital status, image, and other similar information when associated with a person.

Schedule 1 of the Act lists the ten principles for the protection of personal information.[i] Section 4.7 of Schedule 1 addresses "Safeguards", the 7th principle for the protection of personal information.

On June 18, 2015, the *Digital Privacy Act* was passed into law. The *Digital Privacy Act* included an amendment to PIPEDA that imposed certain obligations on organizations that experienced a breach of their security safeguards (i.e. a data breach) which involved personal information under their control.
This amendment comes into effect on of November 1, 2018.

As laid out in Division 1.1 of the Act, the amendment requires private sector organization to: (1) report data breaches to the Office of the Privacy Commissioner (the "**Commissioner**") in certain circumstances, (2) notify individuals and other organizations affected by the breach, and (3) maintain accurate records for *every* data breach.

I. WHAT IS A BREACH OF SECURITY SAFEGUARDS

The Act defines a data breach or a "**breach of security safeguards**" as the loss of, unauthorized access to, or unauthorized disclosure of, personal information resulting from a breach of an organization's security safeguards, or from a failure to establish those safeguards.[ii]

Failure to establish security safeguards constitutes a breach under the Act, therefore organizations are well advised to heed the advice of the Commissioner[iii] and implement detailed policies and organizational codes of practice to meet their obligations to protect personal information and to help avert, or minimize the impact of, a data breach.

"An organization must report to the Commissioner any breach of security safeguards involving personal information that is under the organization's control if, it is reasonable in the circumstances to believe that, the breach creates a real risk of significant harm to an individual."

II. WHEN TO REPORT A BREACH TO THE COMMISSIONER

An organization must report to the Commissioner any breach of security safeguards involving personal information that is under the organization's control *if,* it is reasonable in the circumstances to believe that, the breach creates *a real risk of significant harm* to an individual.[iv]

According to the Act, "**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.[v]

Organizations must evaluate the *real risk*[vi] of significant harm on a case by case basis, taking into account the sensitivity of the personal information involved in the breach and the probability that the personal information has been/ is/ or will be misused. Additional guidance on how to assess the real risk of significant harm is available here.

A. TIMING AND CONTENTS OF THE REPORT TO THE COMMISSIONER

An organization must submit a report to the Commissioner "as soon as feasible after the organization determines that the breach has occurred".[vii] The report must address the following details: (a) the circumstances of the breach and the cause, if known; (b) the exact or approximate day on which, or the period during which, the breach occurred; (c) the personal information that was affected by the breach, if known; (d) the exact or approximate number of individuals affected by the breach; (e) the steps that the organization has taken to reduce the risk of harm to affected individuals that could result from the breach or to mitigate that harm; (f) the steps that the organization has taken or will take to notify affected individuals of the breach; and (g) the name and contact information of the organization's representative with whom the Commissioner can interact.[viii]

If the organization becomes aware of any new information after having made the report, it may submit it to the Commissioner.[ix]

III. NOTIFICATION OBLIGATION FOR ORGANIZATIONS

A. NOTIFICATION TO INDIVIDUAL

An organization must notify an individual of any breach of its security safeguards involving the individual's personal information under the organization's control as soon as possible after the organization determines that the breach has occurred *if* the breach creates a real risk of significant harm to the individual, unless otherwise prohibited by law.[x]

The notice must contain sufficient information to allow the individual to understand the significance of the breach to him or her and to take steps, if any are possible, to reduce the risk of harm that could result from the breach or to mitigate that harm.

"An organization must maintain a record of every breach of security safeguards that involve personal information under its control for 24 months after the day on which the organization determined a breach has occurred."

1. How to Notify an Individual

An organization must notify an individual directly of a breach of the organization's security safeguards in person, or by phone, mail, or email. If such direct means of notification are not practicable because (i) it would be likely to create further harm to the affected individual, (ii) would likely cause undue hardship for the organization, or (iii) the organization does not have contact information for the affected individual, then the organization may notify the individual indirectly through public communications means such as public announcements and/or through the organization's website and its social media platforms.[xi]

2. Contents of Notice to Individuals

The content of a notice of breach that an organization sends to an affected individual is largely similar to the information it must report to the Commissioner. The notice must contain: (a) a description of the circumstances of the breach; (b) the exact or approximate day on which, or period during which, the breach occurred; (c) a description of the personal information that was affected by the breach, if known; (d) a description of the steps that the organization has taken to reduce the risk of harm that could result from the breach; (e) a description of the steps that affected individuals could take to reduce the risk of harm that could result from the breach or to mitigate that harm; and (f) contact information that the affected individual can use to obtain further information from the organization about the breach.[xii]

B. NOTIFICATION TO ORGANIZATIONS

An organization that notifies an individual of a breach of its security safeguards must also notify any other organization, including a government institution, (together "**Other Organizations**") of the breach as soon as possible after the organization determines that the breach has occurred *if* that organization *believes* that the Other Organization may be able to reduce the risk of harm that could result from the breach or mitigate that harm.[xiii]

IV. REQUIREMENT TO KEEP RECORDS

An organization must maintain a record of *every breach* of security safeguards that involve personal information under its control for 24 months after the day on which the organization determined a breach has occurred.[xiv]

The record must contain "any information that would allow the Commissioner to verify"[xv] that the organization complied with its breach reporting and notification obligations under the Act. Further, the organization must be ready to provide to the Commissioner a copy of, or access to, that record on demand.[xvi]

Given its obligations under the Act, an organization is well advised to maintain the following information for *every data breach event* that involves personal information: (i) the date or estimated date of the breach, (ii) a general description of the circumstances of the breach, (iii) the nature of information involved in the breach, (iv) the date on which the report was sent to the Commissioner, or if no report was sent, a brief explanation of why the breach was determined not to pose a real risk of significant harm and the name of the authorizing officer or director of the organization; (v) the date on which affected individuals and Other Organizations, if applicable, were notified or if no notices were sent, then a brief explanation of why the breach was determined not to pose a real risk of significant harm and the name of the authorizing officer or director of the organization.

"The Commissioner may find an organization guilty of a summary conviction and liable to a fine of up to $10,000 or an indictable offence and liable to a fine of up to $100,000."

V. COMPLAINTS AND WHISTLEBLOWING

Even in the absence of a data breach, an organization's poor privacy practices may be exposed by its own employees[xvii] or any other individual.[xviii] The Act permits employees and individuals to alert the Commissioner that an organization is contravening or is planning to contravene the Act's personal information handling provisions and recommendations.

In fact, PIPEDA protects employees of an organization who: (i) refuse to engage in any activity that contravenes the Act and (ii) commit any acts that would prevent an organization from contravening the Act.

This added exposure should motivate organizations to ensure that their personal information handling practices and policies are readily available and are enforced.

VI. OFFENCE AND PUNISHMENT

An organization can run afoul of the Act in a multitude of ways, including by failing to implement security safeguards for personal information, report a qualifying data breach to the Commissioner, notify affected individuals and organizations of a data breach, and keep accurate records of every breach event that involves personal information. In addition, an organization can be found to contravene the Act if it dismisses an employee for whistleblowing or obstructs the Commissioner's investigation of a complaint.

The Commissioner may find an organization guilty of a summary conviction and liable to a fine of up to $10,000 or an indictable offence and liable to a fine of up to $100,000.[xix]

VII. CONCLUSION

Canada respects the privacy of individuals' personal information and is now imposing additional strict obligations on private sector organizations to protect the personal information in their care. The new reporting, notification, and record-keeping requirements are coming into force on November 1, 2018. Organizations are advised to implement or update their personal information handling practices to ensure they comply with PIPEDA and avoid committing an offence under the Act.

[i] https://www.canlii.org/en/ca/laws/stat/sc-2000-c-5/latest#SCHEDULE_1__150607
[ii] *Personal Information Protection and Electronic Documents Act* (S.C. 2000, c. 5) "**PIPEDA**", Section 2(1).
[iii] *Ibid*., Section 24(c).
[iv] *Ibid*., Section 10.1(1).
[v] *Ibid*., Section 10.1(7).
[vi] *Ibid*., Section 10.1(8).
[vii] *Ibid*., Section 10.1(6).
[viii] Breach of Security Safeguards Regulations SOR/2018-64, PIPEDA, Section 2(1).
[ix] *Ibid*., Section 2(2).
[x] PIPEDA Section 10.1(3)
[xi] Breach of Security Safeguards Regulations SOR/2018-64, PIPEDA, Section 4.5.
[xii] *Ibid*., Section 3.
[xiii] PIPEDA, Section 10.2(1) and (2).
[xiv] *Ibid*, Section 10.3(1) and Breach of Security Safeguards Regulations SOR/2018-64, PIPEDA, Section 6(1).
[xv] Breach of Security Safeguards Regulations SOR/2018-64, PIPEDA, Section 6(2).
[xvi] PIPEDA, Section 10.3(2).
[xvii] *Ibid*., Section 27.1(1).
[xviii] *Ibid*., Section 27(1).
[xix] *Ibid*., Section 28.