CARTERS
BARRISTERS
SOLICITORS
TRADEMARK AGENTS

CHARITY & NFP LAW BULLETIN NO. 429

SEPTEMBER 27, 2018

EDITOR: TERRANCE S. CARTER

MANDATORY BREACH OF PERSONAL INFORMATION REGIME COMES INTO EFFECT NOVEMBER 1, 2018

By Esther Shainblum*

A. INTRODUCTION

On November 1, 2018, Division 1.1 of the *Personal information Protection and Electronic Documents Act* ("PIPEDA")[1], establishing mandatory data breach reporting and recordkeeping requirements, together with the accompanying *Breach of Security Safeguards Regulations: SOR/2018-64* (the "Regulations"), which provide additional details about these obligations, will come into force.[2] On that date, organizations subject to PIPEDA, potentially including certain charities and not-for-profits, will be required to comply with the notification, reporting and recordkeeping obligations set out under the new mandatory breach regime. As, in some situations, charities and not-for-profits could be subject to PIPEDA, they should be aware of these new requirements.

B. BACKGROUND

The *Digital Privacy Act*[3], which contains Division 1.1 of PIPEDA, received Royal Assent on June 18, 2015.[4] The mandatory breach notification and reporting obligations set out in the *Digital Privacy Act* were

* Esther Shainblum, B.A., LL.B., LL.M., CRM, practices in the areas of charity and not-for-profit law, privacy law and health law with the Carters Ottawa office. The author would like to thank Christina Shum, B.M.T., J.D., Student-at-Law, for her assistance in preparing this Bulletin.

[1] SC 2000, c. 5 [*PIPEDA*].

[2] These data breach requirements were previously reported in Esther Shainblum, *September 2017 Charity & NFP Law Update*, "Proposed Breach of Security Safeguards Regulations under PIPEDA", online: Carters Professional Corporation <http://www.carters.ca/pub/update/charity/17/sep17.pdf> and Terrance S Carter, *April 2018*http://www.carters.ca/pub/update/charity/17/sep17.pdf *Charity and NFP Law Update*, "Legislation Update: New Data Breach Reporting Regime under PIPEDA in Force on November 1, 2018", online: Carters Professional Corporation <http://www.carters.ca/pub/update/charity/18/apr18.pdf>.

[3] SC 2015, c 32.

[4] *Supra* note 1, s 10.1(1).

to become effective at a later, then unknown, date. On March 26, 2018, Order in Council 2018-0369 proclaimed that sections 10, 11, 14, 17(1), 17(4), 19 and 22 to 25 of the *Digital Privacy Act* would come into force on November 1, 2018.

On September 2, 2017, a first draft of the Regulations was published in the *Canada Gazette* for a 30-day consultation period.[5] On April 18, 2018 the final Regulations were published in the *Canada Gazette* together with a Regulatory Impact Analysis Statement advising that the Regulations would come into effect on November 1, 2018.[6] Organizations have therefore had about seven months to prepare.

C. MANDATORY BREACH NOTIFICATION AND REPORTING REQUIREMENTS UNDER PIPEDA

When Division 1.1 comes into force, it will require organizations that experience certain types of data breaches to report them to the Office of the Privacy Commissioner of Canada ("OPC") and to notify the affected individuals and, in some cases, third party organizations.

1. What Triggers the Notification and Reporting Obligations

The notification and reporting obligations are triggered when an organization experiences a "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. Organizations will need to understand what these terms mean in order to comply with the statute.

Section 2(1) of PIPEDA defines a "breach of security safeguards" as the loss of, unauthorized access to or unauthorized disclosure of personal information resulting from a breach of or a failure to establish the types of security safeguards organizations should have to protect personal information. In a nutshell, PIPEDA requires organizations to have in place physical, organizational and technical security safeguards appropriate to the sensitivity of the information.[7]

Subsection 10.1(7) of the *Digital Privacy Act* defines "significant harm" as including bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional

[5] Breach of Security Safeguards Regulations, (2017) C Gaz I, 3613.
[6] Breach of Security Safeguards Regulations, (2018) C Gaz I, 701.
[7] PIPEDA, *supra* note 1, Schedule 1, s 4.7.3.

opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property.

Subsection 10.1(8) of the *Digital Privacy Act* sets out a number of factors that are relevant to determining whether a breach of security safeguards creates a "real risk of significant harm" to an individual, including:

- the sensitivity of the personal information involved in the breach;
- the probability that the personal information has been, is being or will be misused; and
- any other prescribed factor. The Regulations do not prescribe any additional factors at this time.

The open-ended language of this provision suggests that organizations are not precluded from considering other factors when determining whether a breach creates a "real risk of significant harm."

D. REPORTING AND NOTIFICATION REQUIREMENTS

If, having regard to the definitions described above, an organization experiences a "breach of security safeguards" involving personal information under its control and it is reasonable in the circumstances to believe that the breach creates a "real risk of significant harm" to an individual ("Serious Breach"), the following obligations are triggered:[8]

- it must report the Serious Breach to the OPC;
- it must notify the affected individual of the Serious Breach;
- it must notify any other organization, a government institution or a part of a government institution of the Serious Breach (such as, for example, the police, a bank or a credit reporting agency), if it believes that the other organization may be able to reduce the risk of harm or mitigate that harm,

[8] PIPEDA, *supra* note 1, ss 10.1(1), 10.1(3), 10.2(1).

or if other prescribed conditions are satisfied. The Regulations do not currently identify any prescribed conditions.

The report to the OPC must be written and provided "as soon as feasible"[9] after the organization has determined that a Serious Breach has occurred.[10] However, the organization may submit updates to the OPC regarding the details in the report if it becomes aware of new information after the report has been submitted.[11] While the Regulations are flexible in that the report to the OPC may be sent "by any secure means of communication,"[12] there are certain minimum content requirements prescribed by the Regulations, as discussed below.

The report must include a description of the circumstances of the breach, and if known, the cause.[13] The report must also provide the day on which or period during which the breach occurred; if unknown, then the approximate period of the breach must be given.[14] Other information that must be provided in the report include a description of the personal information that is the subject of the breach, the number (or approximate number) of individuals affected, and the steps that the organization has taken to reduce the risk of harm to the affected individuals or to mitigate the harm caused.[15] Further, the organization must provide a description of the steps it has taken or is planning to take to notify the affected individuals of the breach. Lastly, the report must contain the name and contact information of a person who can answer the OPC's questions about the breach on behalf of the organization.[16]

Notification to the affected individual must be conspicuous[17] and given "as soon as feasible" to the individual after the organization has determined that the Serious Breach has occurred.[18] There is substantial overlap between the information that must be provided to the OPC and to the affected individuals. The notification to individuals must also contain a description of the circumstances of the

[9] SOR/2018-64, s 2(1) [*Regulations*].
[10] *PIPEDA*, *supra* note 1, s 10.1(2).
[11] *Regulations*, *supra* note 9, s 2(2).
[12] *Ibid*, s 2(3).
[13] *Ibid*, s 2(1)(a).
[14] *Ibid*, s 2(1)(b).
[15] *Ibid*, ss 2(1), (c)-(e).
[16] *Ibid*, s 2(1)(g).
[17] *PIPEDA*, *supra* note 1, s 10.1(5).
[18] *Ibid*, ss 10.1(2), 10.1(6), s 10.2(2).

breach, although the notification does not need to disclose any known cause of the breach.[19] The notification must also disclose the date or period (or if unknown, the approximate period) on which the breach occurred, and a description of the personal information that was the subject of the breach to the extent that it is known.[20] The notification must also outline the steps that the organization has taken to reduce the risk of harm that could result from the breach.[21] Finally, the notification must also provide contact information for the organization that the affected individual can use to obtain further information about the breach. However with respect to the notification, the Regulations do not explicitly require that the contact person must be able to speak on behalf of the organization.[22] Additionally, the notification must provide the individual with steps that he or she may take to reduce the risk of harm or to mitigate harm caused.[23] However, organizations are not required under the Regulations to provide new information to the individual that they become aware of after the notification has been provided.

Under PIPEDA, the organization must notify the individual using the methods as prescribed by its regulations.[24] Under the Regulations, notification must generally be given directly to the individual. However the means of communication is flexible in that an organization may notify the affected individual in person, by phone, mail, or email, or in "any other form of communication that a reasonable person would consider appropriate in the circumstances."[25]

The Regulations also provide for exceptions where direct notification is not required. An organization may provide indirect notification to the affected individual if direct notification would likely cause further harm to the individual, undue hardship to the organization, or if the organization does not have the contact information of the individual.[26] Nevertheless, if notification is given indirectly, it must be given by public communication or a "similar measure that could reasonably be expected to reach the affected individuals."[27]

[19] *Regulations*, *supra* note 9, s 3(a).
[20] *Ibid*, s 3(b)-(c).
[21] *Ibid*, s 3(d).
[22] *Ibid*, *s* 3(f).
[23] *Ibid*, *s* 3(e).
[24] *PIPEDA*, *supra* note 9, *s* 10.1(5).
[25] *Regulations*, *supra* note 9, s 4.
[26] *Ibid*, ss 5(1)(a)-(c).
[27] *Ibid*, s 5(2).

E. RECORDKEEPING REQUIREMENTS

Under the mandatory breach requirements, organizations must keep records of every breach involving personal information under its control, regardless of whether or not it is a Serious Breach.[28] Furthermore, in compliance with the regulations, organizations must retain these records for a minimum period of 24 months, starting from the day the organization determines that a breach has occurred.[29] These records must contain "any information that enables the Commissioner to verify compliance" with the OPC reporting and notification to individual requirements under PIPEDA.[30] Further, the organization must provide the OPC with a copy of, or access to, these records upon the OPC's request.[31]

F. FAILURE TO COMPLY WITH REQUIREMENTS

Failure to comply with the notification, reporting, and recordkeeping regime may result in substantial consequences. The offence and punishment provision in PIPEDA are being updated to include the contravention of the mandatory breach requirements. A person who knowingly violates the mandatory breach requirements under PIPEDA and the regulations, or obstructs the Commissioner or its delegate in its investigation of a compliant or its audit, may be liable to a fine of up to $100,000 for indictable offences or $10,000 for offences that are punishable on summary convictions.[32]

The OPC also may enter into a compliance agreement with an organization[33] and has the authority to include any terms as it sees necessary to ensure the organization's compliance with the Act.[34] In the event that an organization does not follow the agreement, the OPC may also seek a mandatory order from the Federal Court to require compliance.[35] Entering into a compliance agreement with the OPC does not protect the organization from prosecution for an offence, nor does it protect the organization from potential legal action by an individual.[36]

[28] *PIPEDA*, *supra* note 1, s 10.3(1).
[29] *Regulations*, *supra* note 9, s 6(1).
[30] *Ibid*, s 6(2).
[31] *PIPEDA*, *supra* note 1, s 10.3(2).
[32] *Ibid*, s 28.
[33] *Ibid*, s 17.1(1).
[34] *Ibid*, s 17.1(2).
[35] *Ibid*, s 17.2(2).
[36] *Ibid*, s 17.1(4).

G. CONSULTATION ON MANDATORY BREACH REPORTING GUIDANCE

The OPC released a draft guidance ("Guidance") with respect to the mandatory breach requirements on September 17, 2018, inviting interested stakeholders to provide comments up until October 2, 2018.[37] In the Guidance, the OPC provided additional comments that supplement the legislative and regulatory provisions.[38] Among other things, the Guidance advises that the mandatory breach requirements apply to all businesses that meet the PIPEDA requirements, regardless of the size of the organization. It also provides examples of various methods of indirect communication that would be acceptable when notifying an individual of a Serious Breach. With respect to this, the Guidance notes that public announcements such as advertisements in online or offline newspapers or a prominent notice on an organization's website would be acceptable. It also advises that the organization should "use a method that is likely to reach affected individuals," and to use measures that the organization would normally use for public announcements.

The Guidance also clarifies that an organization is considered to be in control of personal information, and therefore required to report a Serious Breach if the information is in its possession or custody, even if the personal information has been transferred to a third party for processing. In such cases, the organization that transferred the personal information to the third party remains accountable for it and would be responsible for reporting a Serious Breach to the OPC. In the event that more than one organization is involved with a Serious Breach concerning the same information, each organization is expected to provide its own report to the OPC.

The Guidance recommends that organizations develop a framework for assessing the "real risk of significant harm." With respect to what "sensitivity" means in the context of determining whether a breach carries a "real risk of significant harm," the Guidance refers to PIPEDA Principle 4.3.4 under Schedule 1 of the Act, which states:

[37] Office of the Privacy Commissioner of Canada, "Commissioner seeks feedback on breach reporting guidance" (September 17, 2018), online: *Office of the Privacy Commissioner of Canada* <https://www.priv.gc.ca/en/opc-news/news-and-announcements/2018/an_180917/>.
[38] Office of the Privacy Commissioner of Canada, "What you need to know about mandatory reporting of breaches of security safeguards" (September 17, 2017), online: *Office of the Privacy Commissioner of Canada* <https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/consultation-pb/gd_pb_201809/>.

> …Although some information (for example, medical records and income records) is almost always considered to be sensitive, any information can be sensitive, depending on the context. For example, the names and addresses of subscribers to a newsmagazine would generally not be considered sensitive information. However, the names and addresses of subscribers to some special-interest magazines might be considered sensitive.[39]

The Guidance goes on to advise that, in determining the "sensitivity" of personal information, it is important to look at what personal information has been breached as well as the circumstances.

With respect to the other factor – probability of misuse – the Guidance suggests a number of questions organizations should be asking themselves in determining whether there is a "real risk of significant harm", including who accessed the personal information (known or unknown entities), was it lost, inappropriately disclosed or stolen, has the personal information been recovered, was there evidence of malicious intent and was the personal information encrypted, anonymized or otherwise not easily accessible.

With respect to the recordkeeping requirements, the Guidance provides clarity on the minimum content that the OPC expects to see in organizations' records of data breaches, including, if the breach was not reported to the OPC, a brief explanation of why the breach was determined not to pose a "real risk of significant harm."

The Guidance also includes a draft breach report form designed to make it easier for organizations to report a Serious Breach to the OPC.

H. CONCLUSION

All organizations subject to PIPEDA will be impacted by the new mandatory reporting regime. PIPEDA applies to every organization, including charities and not-for-profits, in respect of the personal information that it collects, uses or discloses in the course of commercial activities. Whether an organization can be said to collect, use or disclose personal information in the course of a commercial activity will vary

[39] *PIPEDA*, *supra* note 1, Schedule 1, Principle 4.3.4.

depending on the facts of each case and charities and not-for-profits should not assume that they are exempt from PIPEDA.

Charities and not-for-profits who have control over personal information of individuals should continue to review and revise their privacy policies in order to ensure that they continue to be consistent with best practices and with new developments in this area of the law.

CARTERS

Carters Professional Corporation / Société professionnelle Carters Ottawa · Toronto
Barristers · Solicitors · Trade-mark Agents / Avocats et agents de marques de commerce Mississauga · Orangeville
www.carters.ca www.charitylaw.ca www.antiterrorismlaw.ca **Toll Free: 1-877-942-0001**

00321978.DOCX