PIPEDA's Breach Of Security Safeguards Regulations Now Published And Open For Comments

September 08, 2017

On June 15, 2015, Bill S-4, the Digital Privacy Act amended the *Personal Information Protection and Electronic Documents Act* ("PIPEDA"). Under new sections 10.1 through 10.3 which are not yet in force, the *Digital Privacy Act* introduces an explicit obligation to notify individuals in cases of breaches, and report to the Office of the Privacy Commissioner of Canada ("OPC"), "if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to an individual." Additionally, an organization notifying an individual in the event of a breach must also notify any other organization that may be able to mitigate harm to affected individuals and must maintain a record of any data breach that the organization becomes aware of. Bill S-4 allows for additional specifications to be provided via regulations.

A consultation process was then undertaken by the government when preparing these regulations which included the publication of a Consultation Document in March 2016 and A Summary of Consultation Responses in October 2016.

The *Breach of Security Safeguards Regulations* ("Regulations") were finally published on September 2, 2017, along with a Regulatory Impact Analysis Statement which can be found in the Canada Gazette. The proposed Regulations are open for comments for a period of 30 days. They will come into force at the same time as section 10 of the *Digital Privacy Act.*

Regulations Objectives

The Regulations are meant to ensure that all Canadians will receive consistent information about data breaches that pose a risk of significant harm to them and that breach notifications contain sufficient information to enable individuals to understand the significance and potential impact of the breach. They are also meant to ensure that the OPC receives consistent and comparable information about data breaches that pose a risk of significant harm and can therefore provide more effective oversight and verify that organizations are complying with these new breach notification requirements.

Requirements for Reporting to the OPC

Section 2 of the Regulations introduces requirements pertaining to content, form and manner for reporting a breach to the OPC. A report of a breach of security safeguards must be in writing and must contain:

- 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; and
- the name and contact information of a person who can answer, the OPC's questions about the breach on behalf of the organization.

These requirements come as no surprise as they essentially mirror the information to be included in a Privacy Breach Incident Report, as recommended by the OPC.

Requirements for Notifying the Affected Individuals

Section 10.1(4) of the *Digital Privacy Act* provides: "The notification shall contain sufficient information to allow the individual to understand the significance to them of the breach and to take steps, if any are possible, to reduce the risk of harm that could result from it or to mitigate that harm. It shall also contain any other prescribed information."

Content of Notification

Sections 3 to 5 of the Regulations provide that such notification provided by an organization to an individual affected by a breach of security safeguards must also contain:

- 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 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; and
- information about the organization's internal complaint process and about the affected individual's right to file a complaint with the OPC.

These requirements are also rather standard and it would appear to be good business practice for organizations affected by a breach to follow this section of the proposed Regulations if they choose to notify affected individuals up until the new sections come

into force. Moreover, these requirements essentially mirror the information to be included in a notification to affected individuals as recommended by the OPC in its Key Steps for Organizations in Responding to Privacy Breaches. In this Key Steps document, the OPC further recommends that sources of information designed to assist individuals in protecting against identity theft (*e.g.*, online guidance on the Office of the Privacy Commissioner's website and Innovation, Science and Economic Development Canada website) also be included in such notification.

Direct vs. Indirect Notifications to Individuals

Direct Notification:With respect to the manner in which organizations must give direct notification to individuals, section 4 of the Regulations specify that direct notification is to be given to the affected individual: (i) by email or any other secure form of communication if the affected individual has consented to receiving information from the organization in that manner; (ii) by letter delivered to the last known home address of the affected individual; (iii) by telephone; or (iv) in person.

We note that the requirement that consent for email notifications must have been obtained by the affected individual, parallels the requirement detailed in the Guidelines for Privacy Breaches of the Government of Canada under the *Privacy Act,* which states that "The institution should use electronic mail only when the individual has previously consented to the receipt of electronic notices." A similar requirement is also included in certain U.S. state laws pertaining to breach notification. An email notification may, at least in some situations, be the best method to notify individuals. Hopefully, the notion of "consent to receive electronic notices" will therefore be interpreted in a flexible manner, as including an implicit form of consent – for example in situations where an individual provided his/her email address to the organization and email is the preferred communication method between the parties.

Indirect Notification:The *Digital Privacy Act* also provides that the notification shall, in prescribed circumstances, "be given indirectly in the prescribed form and manner." Section 5 of the proposed Regulations suggests that indirect notification may be given to the affected individual by an organization if giving direct notification would cause further harm to the affected individual, if the cost of giving direct notification is prohibitive for the organization or if the organization does not have contact information for the affected individual (or the information that it has is out of date). When indirect notification is authorized, the Regulations require that it be provided either by 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

The proposed Regulations also address the record-keeping requirements, as the *Digital* Privacy Act requires organizations to keep and maintain a record of every breach of security safeguards involving personal information under their control "in accordance with any prescribed requirements". Section 6 of the proposed Regulations states that an organization must maintain a record of every breach of security safeguards for 24 months after the day on which the organization determines that the breach has occurred, and that the record must contain any information pertaining to the breach that enables the OPC to verify compliance. The Regulations also specify that a breach report

to the OPC may be used by the organization as a record of the breach of security safeguards.

Conclusion

The publication of these Regulations seem to indicate that new sections 10.1 through 10.3 introduced through the *Digital Privacy Act* should come into force in the near future. Since these proposed Regulations are open for comments for a period of 30 days, organizations should consider submitting their concerns within the prescribed period. Additionally, organizations should also finalize their breach incident response plans and prepare for the coming into force of this new breach notification requirement, especially given that organizations that fail to report breaches as prescribed by PIPEDA, or to keep required records, will be subject to monetary penalties.

Expertise

Cybersecurity, Privacy & Data Protection
