White Paper

*Personal Information Protection and Electronic Documents Act (PIPEDA)*

Understanding PIPEDA Breach Response Obligations

Yardi is committed to protecting the privacy of individuals and achieving and maintaining the trust of its clients. We know that many of our Canadian clients have questions about the new *Personal Information Protection and Electronic Documents Act (PIPEDA)* breach response reporting, notification, and record keeping requirements. To support your PIPEDA compliance efforts, we outline a few notable provisions of the PIPEDA breach response requirements below.

**What are the New PIPEDA Breach Response Obligations?**

On November 1st 2018, new breach response obligations took effect for organizations subject to the PIPEDA. These breach response obligations require organizations to comply with record keeping, reporting, and notification rules if security safeguards for personal information are breached. Mandatory reporting is to the Office of the Privacy Commissioner of Canada (OPC) and notification is to any affected individual whose personal information was compromised. Organizations should consult with their legal counsel about the potential penalties for non-compliance with these rules as well as any updates or changes to these rules.

**What is a breach of security safeguards?**

*PIPEDA* requires organizations to establish security safeguards that “protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification.” Security safeguards include:

- physical measures, including restricted access to offices and filing cabinets;
- organizational measures, such as limiting access privileges or imposing policy-based rules on employees; and
- technological measures, which may include the use of passwords and encryption.

The required security safeguards are not specified by the statute. The only explicit security safeguard required by the statute relates to information and instruction (*i.e.*, the statute requires that organizations “make their employees aware of the importance of maintaining the confidentiality of personal information”).

**When do I Report a Breach to the OPC?**

An organization must report a breach to the OPC if it is reasonable in the circumstances to believe that a breach of security safeguards creates a “real risk of significant harm” to an individual.

The OPC has provided guidance on the test for reporting breaches. The existence of a real risk of significant harm is determined by assessing the “sensitivity of the personal information” involved and “the probability that the personal information has been, is, or will be misused.” But it is important to note that a mere vulnerability or exposure of data does not necessarily constitute a breach of security safeguards. It is always important for organizations to consult their legal counsel for guidance.

According to the OPC, 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.
When are Breaches Reported to the OPC? Who is Responsible for Reporting a Breach?
Organizations must report a breach to the OPC “as soon as feasible” after the breach, even if not all information (e.g. information setting out the cause or indicating the degree of exposure) is known or confirmed. An organization can add or correct information as necessary.

PIPEDA’s accountability principle provides that an organization remains responsible for the personal information it transfers to a third party for processing and, in that context, the party who transfers the data for processing remains the “Principal Organization”. According to the OPC guidelines, the Principal Organization is ultimately responsible for breach reporting in respect of a breach that occurs with a third party processor.

When and How Should Affected Individuals be Notified?
The standard for notifying affected individuals is the same as the standard for reporting to the OPC; notification is required if it is reasonable in the circumstances to believe that a breach of personal information security safeguards creates a “real risk of significant harm” to that individual. As with the reporting requirements, notifications must be given “as soon as feasible” and, again, the Principal Organization is responsible for issuing the required notices to affected individuals.

The notification must include enough information to allow the individual to understand the significance of the breach to the individual and to take steps, if any are possible, to reduce the risk of harm that could result from the breach or mitigate the harm.

The notification must include:
- a description of the circumstances of the breach;
- the day on which, or period during which, the breach occurred or, if neither is known, the approximate period;
- a description of the personal information that is the subject of the breach to the extent that the information is known;
- a description of the steps that the organization has taken to reduce the risk of harm that could result from the breach;
- 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
- contact information that the affected individual can use to obtain further information about the breach.

Generally, an affected individual must be notified directly by telephone, mail, email, or any other form of communication that a reasonable person would consider appropriate in the circumstances. However, in certain circumstances an organization may indirectly notify affected individuals. Indirect notification must be given by public communication or similar measure that could reasonably be expected to reach the affected individuals.

Under what Circumstances Should Third Parties be Notified?
An organization must also notify any government institution or organization if it is reasonable in the circumstances to believe such notification could mitigate the harm, or reduce the risk of harm, that could result from the breach. Notification to law enforcement and payment processors (in credit card breaches) are obvious examples where third-party notification should be exercised.

What Breach Investigation Records Must be Kept?
All PIPEDA-subject organizations are required to keep a record of every breach of security safeguards involving personal information under their control regardless of whether the reporting and notification requirement is
triggered. The records must contain any information that enables the OPC to verify the organization’s compliance with PIPEDA’s reporting and notification requirement.

The OPC has released guidance indicating that it expects organizations to, at minimum, include the following in the record kept:

- date or estimated date of the breach;
- general description of the circumstances of the breach;
- nature of information involved in the breach;
- whether or not the breach was reported to the Privacy Commissioner of Canada/individuals were notified; and
- if the breach was not reported to the Privacy Commissioner/individuals, a brief explanation of why the breach was determined not to pose a “real risk of significant harm.”

The records must be kept for two years and the organization must provide the OPC access to a breach record, or a copy of it, upon request.

**Best Practice: Develop an Incident Response Policy Before a Breach**

Canada’s new mandatory breach reporting requirements emphasize the need for a well-reasoned incident response plan. Yardi clients should implement or, as necessary, update their incident response plans based on the PIPEDA breach response obligations to ensure their policies are designed to help comply with applicable investigation and breach reporting obligations.