Confidentiality Incidents (CIs) (Data Breaches)
Quebec's Private Sector Privacy Law Amendments c. 25
Sections 3.5 to 3.8

Introduction

On September 22, 2021, Quebec passed *An Act to modernize legislative provisions as regards the protection of personal information* (2021, c. 25) ("the Act") updating public and private sector privacy laws. The provisions of the Act come into force over a period of 3 years.

This document was created by leading Canadian privacy experts working with national and regional industry associations. We believe a harmonized approach to privacy law across Canadian jurisdictions is important so that the rules are understandable for individuals and enterprises. Interpretations of privacy laws should be pragmatic, reasonable and focus on the privacy outcomes for individuals and practical implementation for enterprises. With this in mind, we have created what we think is appropriate guidance for interpreting some of the more challenging provisions of the Act.

This document can be shared and used by enterprises. This is not legal advice; it is suggested best practices for entities wishing to work pragmatically on their compliance with the Act before any additional guidance from the *Commission d'accès à l'information* (the "CAI") or regulations are made available. We encourage enterprises to monitor developments in CAI and government guidance on these and other topics related to the Act.

Confidentiality Incidents (CI)

The Act requires enterprises to notify the CAI and affected individuals if a **CI** meets the threshold of presenting a risk of serious injury. Enterprises may also notify third parties who could reduce the risk of injury. Enterprises are required to take reasonable steps to mitigate the impact of incidents, prevent their re-occurrence and to keep a registry of incidents.

The provisions relating to CIs come into effect on **23 September 2022**.

The CI requirements in the Act are substantially similar to the breach regime found in *PIPEDA* and reflected in the processes of many enterprises already complying with *PIPEDA*. It is therefore useful to rely on *PIPEDA*, related Regulations and the Office of the Privacy Commissioner's ("OPC") guidance for assistance in interpreting the Act.

a) What is a CI? (s. 3.6)

The definition of a CI is nearly identical to the concept of a "breach of security safeguards" in *PIPEDA*.

A CI results from:

- access not authorized by law to personal information;
- use not authorized by law of personal information;
- communication not authorized by law of personal information;
- unauthorized use of personal information; or
- loss of personal information or any other breach of the protection of such information.

b) When does an enterprise have to provide notice of a CI? (s.3.5, 3.7)

An enterprise must provide notice of a CI "If the incident presents a risk of serious injury…" It only makes sense for the risk to be real before notifying the CAI or impacted individuals, and so we expect the CI notice threshold to be the same as PIPEDA's "real risk of significant harm" based on the CAI's existing declaration of security incident form questions and examples. The OPC's decisions and guidance on "real risk of significant harm" provides useful insight into the threshold for notification for the Act.

Factors for assessing the risk of serious injury include: sensitivity, anticipated consequences, likelihood of use for injurious purposes (s.3.7). These factors are similar to the harms listed in *PIPEDA* s.10.1(7): 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.

c) Who gets notice of a CI? (s.3.5)

If a CI meets the threshold of presenting a risk of serious injury, notice **must** be given to the CAI and "any person whose personal information is concerned by the Incident" unless the notifications would hamper an investigation conducted by a person or body responsible by law for the prevention, detection or repression of crime or statutory offences.

The enterprise **may** notify any other person or body without the individual's consent to reduce the risk of harm.

d) Form, Content and Terms of Notice of CI (s.3.5)

The form, content and terms of notice will be specified in Regulations. The CAI has previously published guidance on providing notice of a CI, but this guidance is likely to be refreshed as a result of the Act.

For form and content, it is reasonable to rely on:

- For notice to individuals: PIPEDA Breach Regs s.3 and the CAI guidance on page 6, step 4

- For notice to the CAI: PIPEDA Breach Regs s.2 , OPC forms and the voluntary declaration of security incident form currently available on the CAI website

For notice timelines:

- Both the Act and *PIPEDA* use similar standards, "promptly" in the Act and "as soon as feasible" in *PIPEDA*. The OPC guidance should be helpful in determining timelines.

- The the Act timeline applies only to the notice to the CAI. There is no timeline for the notice to individuals or to the person or body that could reduce the risk. Best practice would be to apply the same PIPEDA standard of "as soon as feasible" for notices to individuals or third parties who can help mitigate the risk of harm.

e) Duty to Mitigate (s.3.5)

If an organization believes a CI has occurred, it "must take reasonable measures to reduce the risk of injury and to prevent new incidents of the same nature." Reasonable measures are not defined, however, enterprises could rely on OPC Guidance paragraphs 11 and 12 and CAI's published guidance.

f) Incident Registry (s.3.8)

Similar to *PIPEDA*, enterprises are obligated to keep a register of CIs. The content of the register may be specified in Regulations. It appears **all** CIs, not just those meeting the threshold for notification, are included in the register.

We believe it is reasonable to rely on OPC Guidance (see Part 3) for what a registry should contain for each CI or breach:

- date or estimated date of the breach;

- general description of the circumstances of the breach;

- nature of information involved in the breach and impacted individuals;

- whether or not the breach was reported to the Privacy Commissioner of Canada or individuals were notified; and

- an explanation of the organization's assessment, e.g. why there was no notification.