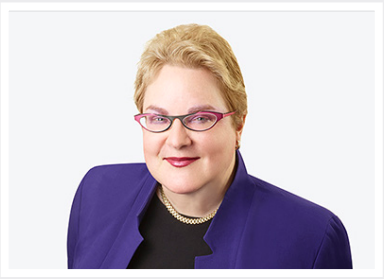
Torkin Manes
Barristers & Solicitors

Torkin Manes LegalPoint

TECHNOLOGY, PRIVACY & DATA MANAGEMENT

MAY 2018

New Rules for Mandatory Privacy Breach Notification in Canada: What Organizations Need to Know



Lisa R. Lifshitz, Partner

PHONE
416 775 8821
EMAIL
llifshitz@torkinmanes.com

Claire Feltrin, Associate

PHONE
416 643 8814
EMAIL
cfeltrin@torkinmanes.com

Background

On April 18, 2018, the final regulations relating to the mandatory reporting of privacy breaches under Canada's *Personal Information Protection and Electronic Documents Act* ("**PIPEDA**") were published. These regulations, which include fines of up to CAD$100,000 for non-compliance, will come into force on November 1, 2018.

Why should organizations pay careful attention to this legislative update? To date, much of the Canadian private sector has not been subject to mandatory privacy breach notification. With the exception of Alberta, data breach reporting under PIPEDA has been voluntary for private sector organizations across Canada. However, the recent amendments to PIPEDA and its regulations (the "**Regulations**") will mean that private sector organizations (except those in the provinces of British Columbia and Quebec) will soon face mandatory breach reporting and record-keeping requirements, which will require organizations to revise internal privacy policies and procedures to ensure compliance with these significant legislative changes.

By way of background, PIPEDA is Canada's federal data protection law, which applies to all private sector organizations regulated by provinces that do not have substantially similar private sector privacy legislation (all provinces except Alberta, British Columbia, and Quebec), that collect, use, or disclose personal information in the course of their commercial activities. PIPEDA also applies to federal works, undertakings and businesses (i.e. airlines, banks, interprovincial railways/trucking, and broadcasting, including the employees of those organizations), and to all personal information that flows across provincial or national borders in the course of commercial transactions.

Below, we provide a brief overview

of the key provisions which organizations should be turning their minds to as the coming into force date approaches.

Breach Notification Provisions in PIPEDA

Overview

In June 2015, Canada passed Bill S-4 – *The Digital Privacy Act* into law. This bill made a number of important amendments to PIPEDA relating to mandatory breach notification and record-keeping. Once these provisions come into force, organizations subject to PIPEDA will be required to report privacy breaches in certain circumstances to affected individuals and to the Office of the Privacy Commissioner of Canada (the "**Commissioner**").

Pursuant to section 10.1 of PIPEDA, organizations will need to notify both individuals (unless prohibited by law) and report to the Commissioner all breaches of security safeguards involving personal information under their control where it is reasonable to believe that the breach creates a "real risk of significant harm to the individual" (we refer to this legal test as the "notification threshold"). This must be done "as soon as feasible" after the organization determines that the breach has occurred, and the notification to affected individuals and report to the Commissioner must contain certain prescribed information, as noted below.

In determining whether the above notification threshold has been met, there are a number of definitions that organizations must keep in mind. A "breach of security safeguards" for instance means the loss of, unauthorized access to, or unauthorized disclosure of personal information resulting from: a) a breach of an organization's security safeguards (referred to in clause 4.7 of Schedule 1), or b) a failure to establish those safeguards. The term "significant harm" on the other hand includes, among other harms, humiliation, damage to reputation or relationships, and identity theft. A "real risk" will require the consideration of such factors as the sensitivity of the information, the probability of misuse, and any other prescribed factor.

Content and Manner of Report to the Commissioner

The report to the Commissioner must be in writing and be submitted by any secure means of communication. The Regulations require this report to contain certain information, including but not limited to a description of the circumstances of the breach and, if known, the cause; a description of the steps that the organization has taken to reduce the risk of harm to affected individuals or to mitigate that harm; and a description of the steps that the organization has taken or intends to take to notify affected individuals of the breach. The Regulations also consider that an organization may not have all the information it needs at the time that a report is made, and as such, explicitly allow an organization to submit new information to the Commissioner after the initial report has been turned in. This is one important change that has been implemented by legislators since the draft regulations were released in September 2017.

Content and Manner of Notification to Affected Individuals

The notification to affected individuals must 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. The notification must also contain certain information, such as a description of the circumstances of the breach and the personal information that was affected, the steps the organization has taken to reduce the risk of harm that could result from the breach, and contact information that affected individuals can use to obtain further information about the breach.

With respect to the manner of notification, notification must be conspicuous and given directly to the affected individuals either by phone, mail, email, in person, or by any other form of communication that a reasonable person would consider appropriate in the circumstances. In prescribed situations, however, *indirect* notification will also be acceptable.

Organizations may give indirect notification to affected individuals where direct notification would be likely to cause further harm to the affected individual, cause undue hardship to the organization, or where the organization does not have contact information for the affected individual(s). This form of notification must be given either by public communication or similar measure that could reasonably be expected to reach the affected individuals. That said, while organizations may be tempted to rely on indirect notification in order to avoid the costs associated with notifying individuals directly, it is not yet clear whether such public communications will be considered by regulators to be a reasonable method of communication in practice.

Notification to Other Organizations

In addition to notifying affected individuals and the Commissioner, it is important to note that PIPEDA will now require organizations to notify a third group, namely government institutions or other organizations if the organization believes that the institution or other organization may be able to reduce or mitigate the risk of harm to the affected individuals.

Mandatory Record-Keeping for all Breaches

Additionally, PIPEDA will now require organizations to keep and maintain records of all breaches of security safeguards. This means that regardless of whether the breach notification threshold is triggered, an organization must maintain a record of every such breach for a period of 24 months from the day that the organization determines that a breach occurred. These records must be provided to the Commissioner upon request and they must contain sufficient information to allow the Commissioner to verify compliance with PIPEDA's breach reporting provisions. Organizations should not ignore this new record-keeping provision, particularly in light of the financial penalties they will soon face for non-compliance.

Enforcement and Penalties

In order to enforce these new breach reporting and record-keeping requirements, PIPEDA now includes financial penalties. Specifically, if an organization knowingly violates either of these requirements, it will face fines of up to CAD$100,000. While these financial penalties in no way come close to the prospective penalties under the European General Data Protection Regulation (GDPR), they clearly 'add teeth' to the above-noted requirements.

Conclusion

The introduction of mandatory privacy breach notification, reporting, and record-keeping under PIPEDA will require organizations to review, revise, and implement new privacy policies and procedures prior to November 2018 to ensure compliance with the above-noted Regulations. The legal threshold for breach notification and reporting must be carefully considered and organizations should consider creating a breach response plan in advance of any breaches. Finally, a fine-tuned record keeping system will be crucial to ensuring that all breaches of security safeguards are recorded in a thorough and consistent manner.

If you have any questions or need advice on the creation or review of your cybersecurity response plan, a member of Torkin Manes' Technology, Privacy and Data Management Group would be pleased to help.