Canada amends PIPEDA

Date : July 28, 2015

On June 18th, Canada enacted amendments to the *Personal Information Protection and Electronic Documents Act* (PIPEDA)bringing into force new obligations for organizations subject to PIPEDA. Many readers of Focus will recall the amending legislation, from its introduction last year (see Canada amends privacy law with introduction of Bill S-4 - Digital Privacy Act). Referred to as the *Digital Privacy Act*, the amending legislation introduces a number of changes that will impact employers, including new mandatory reporting requirements for breaches of security safeguards, as well as other changes to the way in which organizations collect, use and disclose personal information.

Employment-related amendments

The definition of "personal information" under PIPEDA has been modified to remove the former exemption regarding the "name, title or business address or telephone number of an employee" such that this information is now considered "personal information". The application of Part I of PIPEDA, which provides for the protection of personal information, has also been expanded to apply to applicants for employment.

In addition, there are two new exemptions to the consent requirements that apply to employment matters. Employers no longer require the consent of an individual before they can collect, use and disclose personal information for the purposes of establishing, managing or terminating an employment relationship, so long as the individual is informed that the information will or may be used for these purposes. Similarly, where "business contact information" is collected, used and disclosed solely for the purpose of communicating with the individual in relation to their employment, business or profession, consent is no longer required. The amendments define "business contact information" to include name, title, work address and telephone number, and work electronic address.

New obligations to report regarding "breach of security safeguards"

New reporting and recording obligations in the event of breaches of security safeguards do not have immediate effect but will come into force on a day to be fixed by order of the Governor in Council. Nevertheless, organizations are well-advised to establish breach response protocols in preparation for these new requirements.

When these amendments come into force, organizations will be required to keep records of any "breach of security safeguards" that result in a "real risk of significant harm" to the individual to whom the personal information relates and to report these to the Privacy Commissioner. Unless otherwise prohibited by law, the organization will also be required to promptly report any such

breach to the individual to whom the information relates in order to allow him or her to take steps to reduce the risk of harm. Organizations will also be required to notify other organizations or government institutions (without the consent of the individual) if those other organizations may be able to reduce the risk of harm to the individual. The term “breach of security safeguards” is defined as the loss of, unauthorized access to, or unauthorized disclosure of personal information resulting from a breach of, or failure to establish, security safeguards. The term “significant harm” is broadly defined to include amongst other things bodily harm, loss of employment and identity theft. In assessing the risk of significant harm, organizations must consider the sensitivity of the information involved in the breach and the probability that the information will be misused (other factors may be prescribed by regulation).

An organization that knowingly contravenes any of these requirements will be guilty of a summary conviction offence and liable to a fine of up to $10,000, or an indictable offence and a fine of up to $100,000.

New exemptions from consent requirements prior to disclosure

The amended act introduces a number of notable exemptions from the knowledge and consent requirements for the disclosure of personal information. These exemptions permit an organization to disclose personal information to another organization without the knowledge or consent of the individual to whom the information relates for the following purposes:

- to investigate a breach of an agreement or contravention (or potential contravention) of a law; and
- to detect or suppress fraud.

New authority for Privacy Commissioner to enter into compliance agreements

Another notable change that organizations should be cognizant of is that the Privacy Commissioner is granted new authority to enter into compliance agreements with organizations that may breach the legislation. The Commissioner is afforded broad authority to include in the agreements any terms it considers necessary and may enforce compliance through a court order.

Given the severe consequences of failing to comply with PIPEDA, organizations are well-advised to take steps to ensure that they are familiar and compliant with these new privacy obligations.

For further information please contact Porter Heffernan at 613-940-2764 or Steven Williams at 613-940-2737.