PIPEDA CHANGES FINALLY PASS

Posted on June 22, 2015

Categories: Insights, Publications

After several failed attempts, Parliament has finally amended the *Personal Information Protection and Electronic Documents Act* ("PIPEDA" or the "Act"). The *Digital Privacy Act* (the "DPA"), which amends PIPEDA, received royal assent on June 18, 2015. Significant changes to PIPEDA include:

1. Breach Reporting

Under the DPA, organizations will be required to notify the Office of the Privacy Commissioner of Canada (the "OPC") and affected individuals of a breach of security safeguards,[1] if it is reasonable to believe in the circumstances that the breach poses a "real risk of significant harm"[2] to the affected individuals. In assessing risk of harm, both the sensitivity of the information and the probability that it will be misused are relevant. Government institutions and other organizations will also have to be notified if they can mitigate or reduce the risk of harm. Furthermore, organizations will be required to keep a record of all data breaches (whether or not they meet the harm threshold described above), and must report all breaches to the OPC upon request. Knowingly failing to report or record a breach will be an offence punishable by fines of up to C$100,000.

The provisions of the DPA relating to privacy breaches have not yet come into force, but will become mandatory once the associated regulations have been enacted.

2. Amendment to the definition of "personal information" and new provisions respecting "business contact information"

Previously "personal information" excluded certain information about an employee of an organization. Pursuant to the changes implemented by the DPA "personal information" now includes any information about an identifiable individual. However, a new definition of business contact information has been added to PIPEDA, and such information is excluded from the application of Part 1 of the Act if the organization collects, uses or discloses such information solely for the purposes of communicating with an individual in relation to his/her employment, business or profession.

3. Changes to Consent

The DPA amends PIPEDA to explicitly state that consent is only valid if it is reasonable to expect that the

individual would understand the nature, purposes and consequences of the collection, use or disclosure of his/her personal information.

In addition, new exceptions to PIPEDA consent requirements have been introduced, which apply to:

- Personal information in witnesses statements related to insurance claims.
- Personal information produced by an individual in the course of his/her employment, business or profession.
- Disclosure for the purposes of communicating with the next of kin or authorized representative of an injured, ill or deceased individual.
- A disclosure to another organization, which is reasonable for the purposes of investigating a past, present or future breach of an agreement or the laws of Canada or a province, if disclosure with knowledge/consent would compromise the investigation.
- A disclosure to another organization, which is reasonable for the purposes of detecting, suppressing or preventing fraud, if disclosure with knowledge/consent would compromise the ability to prevent, detect or suppress fraud.

See also the new exceptions described under #4 and #5 below.

4. Changes affecting employee privacy

The DPA introduces exceptions to the consent requirements in PIPEDA where collection, use or disclosure of personal information is necessary to establish, manage or terminate an employment relationship. However, notice must still be provided to the individual. This amendment brings PIPEDA closer into line with the employee personal information provisions in the *Personal Information Protection Act* (Alberta) and the *Personal Information Protection Act* (British Columbia).

PIPEDA has also been amended to clarify that it applies to job applicants. However, it is important to remember that PIPEDA only applies to employees and applicants of federally-regulated employers.

5. Business Transactions

The DPA introduces exceptions to the consent requirements in PIPEDA in the context of business transactions (broadly defined), provided that certain conditions are met. This change will bring PIPEDA closer into line with similar provisions in the *Personal Information Protection Act* (Alberta) and the *Personal Information Protection Act* (British Columbia).

6. Compliance Agreements

The DPA amends PIPEDA to explicitly allow the OPC to enter into compliance agreements with organizations.

Such agreements may contain any terms that the OPC considers necessary to ensure compliance with Part 1 of the Act.

For more information on the amendments to PIPEDA, or other privacy and data protection issues affecting your organization, please contact any member of McMillan's Privacy Group.

by Lyndsay A. Wasser, CIPP/C, Co-Chair Privacy

1 The DPA defines "breach of security safeguards" as "the loss of, unauthorized access to or unauthorized disclosure of personal information resulting from a breach of an organization's security safeguards that are referred to in clause 4.7 of Schedule 1 or from failure to establish those safeguards."

2 Defined to include "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."

A Cautionary Note

The foregoing provides only an overview and does not constitute legal advice. Readers are cautioned against making any decisions based on this material alone. Rather, specific legal advice should be obtained.

© McMillan LLP 2015