PRIVACY LAWS

By Charles S. Morgan

PRIVACY LAWS

All businesses in Canada are subject to legislation that regulates the collection, use and disclosure of personal information in the course of commercial activity. "Personal information" generally means information about an identifiable individual. The collection, use and disclosure of personal information by private sector organizations and entities within the provinces of British Columbia, Alberta and Québec is regulated by legislation enacted by each of those provinces. Manitoba adopted private sector privacy legislation in 2013, but it is not yet in force. The federal *Personal Information Protection and Electronic Documents Act* (PIPEDA) governs the collection, use and disclosure of personal information in provinces and in the territories that have not yet adopted substantially similar privacy legislation, as well as in the course of inter-provincial and international commercial activities. PIPEDA also applies (regardless of the province) to all federally regulated undertakings (such as banks and telecommunications service providers).

ALL BUSINESSES IN CANADA ARE SUBJECT TO LEGISLATION THAT REGULATES THE COLLECTION, USE AND DISCLOSURE OF PERSONAL INFORMATION IN THE COURSE OF COMMERCIAL ACTIVITY.

These statutory regimes are all generally built upon the following 10 principles that govern the collection, use and disclosure of personal information:

- accountability;
- identifying purposes;
- consent;
- limiting collection;
- limiting use, disclosure and retention;
- accuracy;
- security safeguards;
- openness;
- individual access; and
- challenging compliance.

Unless certain exceptions apply, an individual's knowledge and consent are required to collect, use or disclose his or her personal information. Explicit consent may be required for more sensitive personal information

(e.g., medical or financial information), while implicit consent may be sufficient for non-sensitive personal information (e.g., mailing address). Pursuant to amendments to PIPEDA adopted in 2015, the consent of an individual is only valid if it is reasonable to expect that an individual to whom the organization's activities are directed would understand the nature, purpose and consequences of the collection, use or disclosure of the personal information to which they are consenting. Exceptions to the "consent" requirement include disclosures of personal information in the context of certain business transactions, as defined in the law.

Currently, Alberta's *Personal Information Protection Act* (PIPA) and Manitoba's *Personal Information Protection and Identity Theft Prevention Act* (PIPITPA) are the only general private sector privacy laws in Canada that impose a statutory obligation on private sector organizations to report privacy breaches. Under Alberta's PIPA, organizations must only report (to the Information and Privacy Commissioner of Alberta) privacy breaches that could pose a "real risk of significant harm to an individual." The Information and Privacy Commissioner of Alberta in turn determines whether an organization needs to notify the individuals affected. By contrast, under Manitoba's PIPITPA, an organization is obligated to notify an individual directly (as opposed to notifying a regulator) if his or her personal information is lost, accessed or disclosed without authorization; no specific "harm" threshold applies. Manitoba's PIPITPA is not yet in force. Pursuant to amendments to PIPEDA adopted in 2015 (expected to come into force in 2017), PIPEDA now also contains a breach notification requirement, pursuant to which an organization must report to the Federal Privacy Commissioner any breach of security safeguards involving personal information under its control if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to an individual.

With respect to transfers of personal information to service providers located outside Canada, the "openness" principle under PIPEDA has been held by federal privacy regulators to require that notice of such transfers should be provided to affected individuals. Alberta's PIPA requires that organizations notify individuals if they transfer personal information to a service provider located outside Canada. Québec's privacy legislation requires organizations to take all reasonable steps to ensure that personal information that is transferred cross-border for processing will not be used for new purposes or communicated to third parties without the consent of the individuals concerned.

In addition to general private sector privacy laws, Alberta, Manitoba, New Brunswick, Newfoundland and Labrador, Ontario and Saskatchewan also have specific health privacy legislation to protect personal health information. For example, Ontario's *Personal Health Information Protection Act*, 2004 establishes rules for the collection, use and disclosure of personal health information by health information custodians in Ontario.

Whether PIPEDA or similar provincial legislation is the applicable privacy regime, immediate priorities for most organizations that establish a business in Canada should include:

- the adoption of a privacy compliance strategy that identifies the organization's compliance with the applicable regulatory regimes;
- the adoption of a privacy policy, and personal information management practices, to ensure compliance with applicable privacy laws;
- the appointment of an individual who will be responsible for the administration and oversight of the organization's personal information management practices and who will be prepared to implement any changes required by applicable legislation;
- a review of the current personal information practices of the organization outside Canada and proposed information practices within Canada, including determining what personal information is collected, and from where; what consents are obtained and what purposes are identified when collecting personal information; where personal information is stored; how personal information is used; when and to whom personal information is disclosed; and how current personal information practices of the organization may need to be changed for the collection, use and disclosure of personal information in Canada;
- a review of the organization's data management infrastructure to ensure that the infrastructure is adequately flexible and robust to facilitate implementation of the organization's privacy policies and data management practices;

IMMEDIATE PRIORITIES FOR MOST ORGANIZATIONS THAT ESTABLISH A BUSINESS IN CANADA SHOULD INCLUDE THE APPOINTMENT OF AN INDIVIDUAL WHO WILL BE RESPONSIBLE FOR THE ADMINISTRATION AND OVERSIGHT OF THE ORGANIZATION'S PERSONAL INFORMATION MANAGEMENT PRACTICES.

- the implementation of consent language in contracts, forms (including Web forms) and other documents utilized when collecting personal information from individuals (including customers and employees); and
- the requirement, where there are contracts with third parties to whom personal information will be disclosed (or where the third party is granted access to the personal information), that the third party agree to appropriate contractual terms, such as: specifying the ownership of the data and ensuring that the third party will provide adequate security safeguards for the information; ensuring that the personal information will be used only for the purposes for which it was disclosed to the third party; ensuring that the third party will cease using (and return or destroy) the personal information if requested; and providing for indemnification by the third party for any breach of such terms.

Implementation of such initial steps may require several months, depending on the size and maturity of the organization.

Compliance with privacy laws needs to be considered in any business transaction involving the disclosure or transfer of personal information, such as purchases or sales of businesses, outsourcing transactions and securitization transactions. For example, when contemplating the purchase of a business in Canada, it is essential that a review of the privacy policies and practices of the target form part of the due diligence process. If personal information of employees or customers has to be disclosed to the purchaser during the due diligence process, it is also essential that an appropriate confidentiality regime be established for the process. It is recommended that only personal information that is necessary or likely to affect the decision to proceed with a transaction or its terms (including price) be disclosed.

Failure to comply with privacy laws can result in complaints to the relevant Privacy Commissioner, orders and fines. An organization with deficient privacy practices may risk adverse publicity for failure to comply with privacy laws.

In light of the complexity of privacy laws and the differences between the various laws that may apply to an organization or to a particular business unit, ensuring privacy compliance across an organization's departments may be challenging, particularly for organizations that operate globally.

FOR MORE INFORMATION, PLEASE CONTACT:

Charles S. Morgan
514-397-4230
cmorgan@mccarthy.ca