PALLETTS
Pallett Valo, LLP
Lawyers & Trade-Mark Agents

Privacy Law

June 2004

Privacy Law – What it means to your business

Effective January 1, 2004, the *Personal Information Protection and Electronic Documents Act* ("PIPEDA"), began to apply to all organizations in Ontario dealing with an individual's personal information in the course of a commercial activity.

What is PIPEDA?

PIPEDA was enacted to prohibit the collection, use or disclosure of personal information about an identifiable individual unless informed consent is obtained from that individual. The legislation aims to provide assurances to the public that personal information will be collected, used or disclosed only for clearly defined purposes, which purposes a reasonable person would consider appropriate in the circumstances. Organizations must inform individuals what personal information is being collected and how it will be used or disclosed.

Organizations must obtain consent from the individual to the collection, use and disclosure of such personal information. Additional consent must be obtained if the organization later wishes to use or disclose the personal information for new or secondary purposes.

Consent can be expressly given, or it can be implied from a certain form of conduct. In obtaining consent, organizations should take into account the sensitivity of the personal information and the context in which the personal information is provided. PIPEDA does not provide any "grandfathering" exception to the consent requirement for personal information already in the possession of an organization when PIPEDA came into force. Therefore, continued use of personal information collected before the applicability of PIPEDA may also require consent.

PIPEDA also regulates the protection, retention and destruction of personal information. It permits individuals to access their personal information, at minimal or no cost, and to seek corrections to it. If organizations do not comply with PIPEDA, they may be subject to the penalties set out in the statute.

Which provinces are subject to PIPEDA?

PIPEDA has applied to federally regulated organizations such as banks, broadcasters, and airlines since January 1, 2001.

Effective January 1, 2004, PIPEDA began to apply to every business in Canada except those in provinces that have "substantially similar" privacy legislation in place. In such provinces, the provincial legislation would govern commercial activities that are provincially regulated instead of PIPEDA. Provinces such as Quebec, Alberta and British Columbia have already enacted their own private sector privacy statutes. Although PIPEDA currently governs the collection, use and disclosure of personal information in Ontario, there is a strong possibility that the Ontario government will enact its own legislation which will govern the collection, use and disclosure of the personal information of individuals in the province. If Ontario's privacy legislation is found to be "substantially similar" to PIPEDA, then organizations in Ontario will be subject to the provincial privacy legislation as opposed to PIPEDA.

What is personal information?

PIPEDA defines personal information as "information about an identifiable individual" and includes any personal information, recorded or not, in any form, including digital or paper format.

The following are examples of personal information:

- name, home address, home and cellular telephone numbers, email addresses
- gender, age, SIN number, income and blood type
- credit records, loan records, existence of a dispute between a consumer and a merchant, and intentions to acquire goods or services

Personal information may be factual or subjective and does not have to be recorded. PIPEDA also protects personal information of a sensitive nature provided that is collected, used or disclosed in the course of commercial activity, including marital status, racial or ethnic origin, political opinions, religious beliefs, trade union membership and sexual orientation.

What information is not personal information?

Under PIPEDA, the following information is not considered personal information:

- information typically contained on a business card, such as the name, business title, business address, and business telephone of any employee

- information appearing in a registry collected under a statutory authority and to which a right of public access is authorized by law
- information that appears in a record or document of a judicial or quasi-judicial body, that is available to the public
- information that appears in a publication, including a magazine, book or newspaper, in printed or electronic form, that is available to the public where the individual has provided the information

Does PIPEDA apply to your business?

All organizations are subject to PIPEDA to the extent that they collect, use or disclose personal information in the course of a commercial activity. PIPEDA defines "organizations" to include persons, associations, partnerships and trade unions. The term "persons" includes both corporations and individuals.

While PIPEDA might seem to target organizations whose main business is trading or selling personal information, any organization that collects personal information, either in person, by telephone, fax, email, through a website or otherwise, should ensure that it is in compliance with PIPEDA.

Who in Ontario is exempt from PIPEDA?

PIPEDA does not apply to:

- personal information about an individual in the course of his or her employment unless the individual is an employee of an organization that is a federal work, undertaking or business, or unless the employee's personal information is collected, used or disclosed in the course of a commercial activity, such as the sale or exchange of personal information
- information about corporations, organizations, groups or other entities which does not constitute personal information
- provincial and territorial governments and their agents
- personal information about an individual that is collected, used or disclosed strictly by or for another individual's personal purposes or for a journalistic, artistic or literary purpose and for no other purpose

How should your business comply?

Compliance with PIPEDA requires a thorough and thoughtful review of all of an organization's personal information gathering and handling processes, including ongoing activities and new initiatives. For larger organizations, privacy compliance may involve creating a privacy team to analyze the collection, use and disclosure of personal information within the organization, and implementing effective training and monitoring procedures.

The most basic questions that should be addressed in any audit of an organization include: What personal information is collected? How is it collected? How is consent obtained? What is the personal information used for? Where is it kept and for how long? Who has access? What security measures are used? To whom and when is it disclosed? When is it disposed of? How is it disposed of?

The goals of the privacy audit are to ensure that:

- the purposes for which personal information is collected, used and disclosed are reasonable
- informed consent was obtained
- personal information is collected, used and disclosed only for those purposes for which informed consent was obtained, and no other
- personal information is accurate and secure
- personal information is not kept longer than necessary, and is disposed of appropriately
- organizations have a means by which they can access an individual's personal information, if requested, and correct errors regarding the personal information
- procedures are in place if individual challenges the organization's compliance with PIPEDA

All organizations should designate responsibility for a PIPEDA compliance program to someone within the organization, a privacy officer. The privacy officer is accountable to the organization and should be authorized to facilitate compliance with the privacy legislation. The privacy officer will field enquiries or complaints regarding the organization's collection, use and disclosure of personal information. Larger organizations may require a privacy team to work under the privacy officer to ensure that privacy policies are implemented and effective. Members of the privacy team could include employees in management, marketing, human resources, technology and legal departments.

The privacy officer or privacy team should:

- develop a privacy policy for the organization
- put in place internal privacy policies and procedures to ensure personal information is collected, used and disclosed in accordance with PIPEDA
- communicate the privacy policies and procedures to all members of the organization
- educate and train staff to manage and protect the privacy of personal information in accordance with PIPEDA and the organization's privacy policy
- disseminate information about the organization's privacy practices, through brochures or pamphlets, or by posting the organization's privacy policy on its website
- ensure that personal information collected by the organization is kept secure through physical or electronic means
- review the organization's existing contracts and agreements with customers, suppliers, third party service providers and related organizations to ensure that such parties handle all personal information which has been collected by the organization and disclosed to the third party in accordance with PIPEDA
- review the organization's practices relating to the disposal of personal information
- establish mechanisms for responding to inquiries and complaints and to seek resolution of disputes

The privacy officer should be given the resources necessary to understand and implement the legislative requirements. Each organization should communicate the name and title of the privacy officer, both internally and externally.

After an audit has been completed, the privacy officer or team should ensure that a privacy policy is created for the organization, which policy should be communicated to the organization's employees, customers, suppliers and the public. Such policy should comply with the ten "privacy principles" found in Schedule 1 to PIPEDA:

Accountability: An organization is responsible for personal information under its control and must designate an individual or individuals who are responsible for the organization's compliance with these ten principles.

Identifying Purposes: The organization must identify the purposes for which the information is collected at or before the time the information is collected. If the purposes change, the organization must identify the change in purpose.

Consent: The knowledge and meaningful consent of an individual are required for the collection, use or disclosure of personal information, except where to do so would be inappropriate.

Limiting Collection: The personal information collected must be limited to that which is required for the purposes identified by the organization. Information must be collected by fair and lawful means.

Limiting Use, Disclosure, and Retention: Personal information must not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information must be retained only as long as it is required for the fulfillment of those purposes. Procedures should be implemented to govern the destruction of personal information.

Accuracy: Personal information must be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.

Safeguards: Personal information must be protected by security safeguards appropriate to the sensitivity of the information. Methods of protection should include physical measures, organizational measures and technological measures.

Openness: An organization must make available to individuals specific information about its policies and practices relating to the management of personal information.

Individual Access: Upon request, an individual must be informed of the existence, use and disclosure of his or her personal information and shall be given access to that information. An individual should be given the opportunity to challenge the accuracy and completeness of the information and have it amended as appropriate.

Challenging Compliance: An organization must put procedures in place to receive and respond to complaints or inquiries about its policies and practices relating to the handling of personal information. An organization must investigate all complaints.

What are the consequences for non-compliance?

Any organization that fails to comply with PIPEDA faces significant risks, including:

- an individual's refusal to provide personal information
- negative publicity
- damage to the organization's reputation, brand or business relationships
- accusations of deceptive business practices
- customer, supplier, employee or shareholder distrust
- reduced revenue, market share or shareholder value
- industry or regulatory sanctions
- legal liability, including the payment of substantial fines as contemplated by PIPEDA

Who oversees compliance with PIPEDA?

The office of the Privacy Commissioner of Canada is responsible for promoting awareness and assisting individuals and organizations with privacy issues. It is also responsible for overseeing organization's compliance with the requirements of PIPEDA. The Privacy Commissioner plays an ombudsperson role to help identify problems and work with the parties to a dispute in order to reach a resolution. The Privacy Commissioner possesses broad investigative and audit powers under PIPEDA. In particular, the Privacy Commissioner is entitled to audit an organization's personal information management practices where there are reasonable grounds to believe the organization is not fulfilling its obligations under PIPEDA.

PIPEDA allows individuals to complain to the Privacy Commissioner, who must then investigate matters. After receiving an investigation report, the individual or the Privacy Commissioner may bring an application to the Federal Court of Canada for a hearing. If a federal court finds any violation of PIPEDA, it has the ability to provide any of the following remedies:

- order an organization to correct its practices
- publish a notice of any corrective action taken or proposed
- award damages, including damages for humiliation

PIPEDA also contains "whistle-blower" protection. For example, PIPEDA provides for the protection of the identity of a person who notifies the Privacy Commissioner that an organization's privacy practices contravene provisions of PIPEDA. An employee who in good faith and on reasonable belief, either discloses a contravention of PIPEDA or refuses to violate PIPEDA, is protected from discipline or dismissal by the organization.

PALLETTS
Pallett Valo, LLP
Lawyers & Trade-Mark Agents

Why is compliance with privacy legislation a good business practice?

Aside from an organization's legal obligations, on a more practical note, it is simply good business practice to have proper policies and procedures in place to regulate the collection, use and disclosure of personal information. A PIPEDA compliance program helps organizations find out where they are vulnerable, and what they can do to protect themselves. The benefits of conducting a privacy audit and developing good privacy policies and procedures include:

- avoiding a potential fiasco where personal information is inadvertently disclosed without consent, leading to embarrassment of the organization or one of its customers, suppliers or other third parties
- improved accuracy of information in the possession of the Organization
- improved processes for the collection of information
- increased customer confidence
- increased protection of the integrity of the organization's property
- increased customer trust and loyalty
- increased cost savings

How can we help your organization comply?

Pallett Valo LLP's Privacy Group provides legal advice to organizations in connection with conducting privacy audits and developing PIPEDA compliance programs. We can assist your organization in the following ways:

- designing and assisting in the performance of a privacy audit
- analyzing the results of the audit and determining what procedures and policies should be created
- drafting the required privacy policy for your organization
- assisting in the drafting of internal policies and procedures to govern your organization's information handling practices
- drafting or modifying any internal documents or contracts with third parties to ensure compliance with PIPEDA
- conducting employee training and education programs on how to handle personal information
- re-designing application or membership forms, or other information gathering documentation
- re-writing or re-negotiating contracts with service providers who process personal information

The purpose of this document is to provide information as to recent developments in the law. The comments are of a general nature and do not contain a full analysis of the law nor does it constitute an opinion of Pallett Valo, LLP or any member of the Firm on the points of law discussed.

Brian Reiss *is a partner in the firm and a member of the Business Law Group as well as the Privacy Law Group.*

Andy Balaura *is a member of the firm's Management Labour & Employment Group as well as the Privacy Law Group.*

Contact Members Of The Privacy Law Group

Brian Reiss breiss@pallettvalo.com
Direct Dial: 905.273.3022 Ext. 278

Andy Balaura abalaura@pallettvalo.com
Direct Dial: 905.273.3022 Ext. 225

If you would like additional copies of the newsletter, or know of anyone who would be interested in joining our mailing list, please call Lesley Harrington at 905-273-3300