

McLEAN & KERR LLP
BARRISTERS & SOLICITORS

BULLETIN

Proud of our past. Committed to your future.

December 8, 2003

Minding Your Business Is Part Of Your Business - Federal Privacy legislation will govern you on January 1, 2004!

What is PIPEDA?

PIPEDA is an acronym for the “*Personal Information Protection and Electronic Documents Act*”. It is federal privacy legislation that establishes rules with respect to the collection, use or disclosure of personal information. Since 2001, PIPEDA has applied to federally-regulated business (i.e. banks, airlines, telecommunications and transportation companies) and to businesses that collect, use or disclose personal information across provincial and national borders (i.e. credit reporting agencies or “mailing list” exchanges). On January 1, 2004, PIPEDA will apply much more broadly.

What Happens On January 1, 2004 To Businesses In Ontario?

On January 1, 2004 PIPEDA will apply to every Ontario business or organization which collects, uses or discloses personal information in the course of a commercial activity. This legislation will apply until Ontario enacts its own privacy legislation, which must be substantially similar to the federal legislation.

What Is “Personal Information”?

“Personal Information” is defined as “...information about an identifiable individual, but does not include the name, title, or business address or telephone number of any employee of an organization”. For example, information that relates to an individual’s personal characteristics (i.e. gender, age, marital status, unlisted home address, unlisted

home telephone number, income), health (i.e. health history, health conditions, health services received), activities and views (i.e. religion, politics, opinions expressed, opinion or evaluation of an individual, social status or disciplinary actions), intentions (i.e. to acquire goods or services, or change jobs), ID numbers and credit or loan records are all personal information.

Corporations are not protected by privacy legislation, only individuals. Also, some information that is otherwise publicly available is not protected.

What Is A Commercial Activity?

A commercial activity is defined as “...any particular transaction, action or conduct or any regular course of conduct that is of a commercial character”. It specifically includes the selling, bartering or leasing of donor, membership or other fundraising lists.

The above definition leaves it unclear whether PIPEDA will apply to not-for-profit organizations. At this time not-for-profit organizations are generally being advised to comply because the term “commercial character” does not necessarily translate into “for profit” only.

How Does PIPEDA Affect You As An Employer?

PIPEDA governs the employer-employee relationship for federally regulated industries as described above.

Continued...

However, for constitutional reasons, PIPEDA does *not* apply to the personal information of employees in Ontario collected by an employer:

1. that is in a non-federally regulated industry; and
2. does *not* engage in the collection, use or disclosure of this information in the course of a commercial activity (i.e. sells the information).

In other words, PIPEDA will *not* apply to most employers in Ontario in respect of the collection, use or disclosure of personal information about its employees.

Notwithstanding this gap, employers would be well advised from a “best-practices” standpoint to take measures to develop a privacy policy to protect their employees’ personal information in the same way as they will their customers’ personal information.

What Are PIPEDA’s Governing Principles?

PIPEDA’s requirements stem from 10 basic principles, developed by the Canadian Standards Association, which are set out in the legislation. They articulate guidelines for the collection, storage, use and disclosure of personal information.

The principles are:

1. **Accountability** - The organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization’s compliance with the legislation’s privacy principles.
2. **Identifying Purpose** - The purposes for which personal information is collected must be identified by the organization at or before the time the information is collected.
3. **Consent** - The knowledge and consent of the individual are required for the collection, use or disclosure of personal information, except where inappropriate (ie. an emergency situation).
4. **Limiting Collection** - The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.
5. **Limiting Use, Disclosure and Retention** - Personal information shall 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 shall be retained only as long as necessary for the fulfilment of those purposes.

6. **Accuracy** - Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.
7. **Safeguards** - Personal information shall be protected by security safeguards, appropriate to the sensitivity of the information.
8. **Openness** - The organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.
9. **Individual Access** - Upon request, an individual shall be informed of the existence, use and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.
10. **Challenging Compliance** - An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization’s compliance.

How Do You Put These Principles Into Action?

There is no standard privacy policy “template” because of the varying nature of each organization’s businesses and practices. Each organization should examine carefully how to apply the privacy principles in light of its own activities. Here are some suggestions on how to proceed.

1. Select a Chief Privacy Officer (CPO)

The CPO’s role is to oversee the organization’s personal information handling practice. The CPO is responsible for every aspect of the personal information handling practice for the organization and to ensure its practice is in compliance with the 10 principles of PIPEDA. The CPO must oversee the development of the privacy policy and procedure. This will include the design and co-ordination of an internal audit to determine whether the organization’s personal information practice is in compliance with PIPEDA. The CPO handles the

implementation of the privacy policy and procedure once it is in place. Any request for access to or correction of personal information and all complaints are to be handled by the CPO. The CPO should be a person with a measure of seniority and responsibility within the organization.

2. Conduct an internal audit of the organization

Below is a list of suggested questions that should be asked when conducting an internal audit. This list is by no means exhaustive and depending on the nature of your organization's commercial activities, may prompt further questions:

- what personal information is collected?
- for what purposes do we collect the personal information?
- how is the information collected?
- how is consent of the individual obtained (or is it implied)?
- what do we do with the personal information?
- how do we store and safeguard the personal information?
- to whom and under what conditions do we disclose the personal information?
- how do we dispose of the personal information and when do we do so?

3. Develop a privacy policy

An *external* privacy policy must be developed, based on the 10 governing principles outlined above and made available to all customers and clients. Clients can be informed of the organization's privacy policy through a mail-out pamphlet or brochure. If your organization has a web site, a link to the policy should be clearly displayed on your home page as well as on pages which request personal information or provide a link for sending a message. Web accessible organizations should also develop a web site privacy policy to address personal information that is collected through the web site.

Additionally, it would be advisable to develop a further *internal* privacy policy to deal with specifics of collection, storage and handling of personal information within the organization and to set out proper procedures for requests for access.

4. Review agreements with service providers

The organization should review all agreements with their third party service providers who handle or access the personal information collected by or on behalf of the organization to ensure that those persons also comply with PIPEDA in the handling of such information.

5. Ensure consent of the individual is obtained

The organization must obtain an individual's consent when it collects, uses or discloses the individual's personal information. The individual has a right to access personal information held by the organization and to challenge its accuracy. Personal information can only be used for the purposes for which it was collected. If the organization is subsequently going to use it for another purpose, consent must be obtained again for the new purpose. However, consent in some instances may be implied and sometimes consent is not required (i.e. in an emergency).

For personal information already collected, organizations are not required to recollect it. However, in order to continue to use or disclose the information, consent is required. An organization can inform clients what it does with the previously collected information, to whom it is/was disclosed, and give clients the opportunity to object to the continued use or disclosure.

6. Ensure security of personal information

All security policies including physical measures, technical/electronic tools and organizational controls should be tested and evaluated, and changed or implemented where required.

7. Train your staff

Staff have a key role in ensuring that personal information is kept confidential. They should be trained to ensure compliance with privacy policies and handle access and correction requests.

Continued...

What Are The Consequences Of Non-Compliance?

The federal Privacy Commissioner is responsible for ensuring compliance with the Act and will become involved if a complaint is not resolved between the individual and the business organization. The consequences of an organization's failure to comply with PIPEDA may include:

1. an audit of your organization's information management policies by the Privacy Commissioner,
2. award of damages by the courts, and/or
3. fines of up to \$100,000.

Stay Tuned!

Privacy is a developing area of the law. The full impact of PIPEDA and whether the Ontario government will step up to the plate to introduce its own privacy legislation in 2004 is unclear. However, one thing is clear - privacy protection will be an integral part of your business come January 1, 2004.

More Information

If your organization would like assistance in conducting an internal audit, drafting privacy policies for your business, or would like to discuss the implications of PIPEDA for your organization please do not hesitate to contact either:

December 8, 2003

*Christine Renaud
416-369-6606
crenaud@mcleankerr.com*

*Jennifer Searle
416-369-6632
jsearle@mcleankerr.com*

Web site: www.mcleankerr.com

MCLEAN & KERR LLP

BARRISTERS & SOLICITORS

Founded over 75 years ago, McLean & Kerr is a multi-disciplined law firm located in the heart of Toronto. Its clients include individuals as well as local, national and international enterprises and groups requiring a wide range of personal and business assistance.

McLean & Kerr's areas of practice include corporate, commercial, secured lending, commercial real estate, commercial leasing (landlord and tenant), insurance, employment, family, international, securities, mining,

labour, probate and estate administration and litigation in all courts.

In addition, the firm has access, through established relationships, to professional tax advice and counsel in other jurisdictions.

The *Bulletin* is produced by McLean & Kerr for its clients and other interested parties. The contents of the *Bulletin* are necessarily of a general nature and are not intended to be relied upon as legal advice.