AYLESWORTH LLP
BARRISTERS & SOLICITORS

Compliance with the Personal Information Protection and Electronic Documents Act

A PDF version of this Guide is available on our website at:

http://www.aylesworth.com

CLIENT FOCUSED - SINCE 1861
P.O. Box 124, 18th Floor, 222 Bay Street, Toronto, Ontario M5K 1H1
Tel: 416-777-0101 **Fax:** 416-865-1398 **Web:** www.aylesworth.com

AYLESWORTH LLP
BARRISTERS & SOLICITORS

COMPLIANCE WITH THE PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT

INTRODUCTION AND BACKGROUND

On January 1, 2001, Part I of the *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5 ("PIPEDA") came into force. PIPEDA, which was designed to ensure that Canadians will have protection for personal information held by the private sector, was to be implemented in three phases over three years. The final phase of implementation began on January 1, 2004. Presently, PIPEDA applies to every organization across Canada that collects, uses or discloses personal information in the course of commercial activities within a province and to all inter-provincial and international flows of personal information.

Unlike comparable legislation in the United States, PIPEDA is omnibus legislation that applies all across the country. If a province enacts private sector privacy legislation that is found to be substantially similar to PIPEDA, it means that an organization, a class of organizations, an activity or a class of activities to which the legislation applies is exempt from the application of PIPEDA in respect of the collection, use or disclosure of personal information that occurs within that province. If a province enacts private sector privacy legislation that is not found to be substantially similar to PIPEDA, the provincial law will remain operative but effective January 1, 2004, it will operate concurrently with the federal law. With one exception, the federal provisions will take precedence to the extent of any inconsistency and all organizations carrying out commercial activities will have to comply with the provisions of PIPEDA. PIPEDA will continue to apply to flows of personal information across provincial borders.

Quebec's *An Act Respecting the Protection of Personal Information in the Private Sector*, Alberta's *Freedom of Information and Protection of Privacy Act* and British Columbia's *Personal Information Protection Act* are legislation deemed to be substantially similar to PIPEDA and consequently PIPEDA only applies to an organization's collection, use and disclosure of personal information outside each of the respective provinces. Ontario is currently governed by the *Freedom of Information and Protection of Privacy Act* and the *Municipal Freedom of Information and Protection of Privacy Act*, neither of which are deemed to be similar to PIPEDA. The Government of Ontario released draft legislation called the *Privacy of Personal Information Act, 2002*, which has not been enacted as of October 1, 2005.

HOW DOES THIS AFFECT YOU?

If during the course of your business you collect and use personal information and personal information is an important part of your business, you must ensure that your business complies with the requirements of PIPEDA. Compliance with PIPEDA can enhance a company's business reputation by demonstrating that it respects individuals' personal information. And failure to comply can lead to significant financial penalties and loss of the public's trust in your organization.

WHAT ARE THE CONSEQUENCES OF VIOLATING PIPEDA?

PIPEDA created the office of the Privacy Commissioner of Canada (the "Commissioner") to act as ombudsman. Individuals may complain to either the alleged infringing organization or the Commissioner, or the Commissioner may initiate a complaint where a suspected violation of PIPEDA has or is taking place. If a violation of PIPEDA has occurred, an organization may face:

- an audit of the personal information management practices of the organization
- an application to the Federal Court for damages
- an investigation by the Commissioner
- a fine of up to $10,000 (per incident) on a summary conviction or $100,000 (per incident) for an indictable offence
- loss of the data that it collected
- adverse publicity and loss of the public's trust

Under PIPEDA, it is an offence to:

- destroy personal information that an individual has requested
- retaliate against an employee who has complained to the Commissioner or who refuses to participate in a violation of PIPEDA
- obstruct or otherwise refuse to co-operate with the Commissioner in the investigation and resolution of a complaint

WHAT IS PERSONAL INFORMATION?

PIPEDA defines personal information as any factual or subjective information, recorded or not, about an identifiable individual. It includes things such as race, ethnic origin, colour, age, marital status, religion, education, medical, criminal, employment or financial history, credit records or medical records, residential address and residential telephone number, numerical identifiers such as the Social Insurance Number, fingerprints, blood type, tissue or biological sample, and views or personal opinions. The foregoing examples may appear in any form.

Basically, any information about a person that readily identifies that individual beyond their name, title, business address or business telephone number cannot be collected, used or disclosed in the course of commercial activity without that person's knowledge or informed consent.

Before collecting, using or disclosing personal information in the course of commercial activity, the individual(s) must voluntarily agree, either expressly or impliedly, to the collection, use and

disclosure. Express consent is given either verbally or in writing and implied consent is given when the action/inaction of an individual reasonably infers this consent.

Information that is not considered personal is information that is publicly available, such as information found in a telephone, professional or business directory, information found in registries collected under a statutory authority, court records and published personal information that the individual has provided. Such information can be collected, used or disclosed without the individual's knowledge or consent.

DOES THE ACT APPLY RETROACTIVELY?

Although it is not explicitly clear from a reading of PIPEDA whether or not its provisions are intended to apply retrospectively, the prudent view would be that personal data collected prior to the effective date of PIPEDA will be subject to PIPEDA. There is no "grandfathering" of pre-PIPEDA information for the purposes of excluding that information from the provisions and principles of PIPEDA simply because PIPEDA does not make the distinction between pre-PIPEDA information and post-PIPEDA information. Having stated this, however, there appears to be some consensus among lawyers that PIPEDA is not retroactive in the sense that consent must now be obtained in order for the organization to retain personal information previously collected. It must be noted, however, that the retention of personal information already collected must be reasonable and justifiable, otherwise personal information should be purged from databases according to procedures that are in place to govern the secure destruction of personal information. Consent may not be necessary for the past collection of personal information, however, going forward it will be necessary for the use and disclosure of personal information in existing databases no matter how long ago the information was collected. In other words, PIPEDA applies to the subsequent use and disclosure of personal information previously collected, especially if the purposes for which the information was collected have changed. As Canada's Privacy Commissioner has significant discretion in interpreting PIPEDA, it remains to be seen exactly how PIPEDA's retroactivity will be applied. However, at this time, it appears that PIPEDA's application is retroactive in terms of an organization's future use and disclosure of personal information but not in terms of obtaining consent for previously collected information.

HOW TO COMPLY WITH PIPEDA

A business seeking to comply with PIPEDA must abide by the following ten (10) principles set out in Schedule 1 of PIPEDA. These principles are derived from the Canadian Standard's Association's *Model Code for the Protection of Personal Information.* For your convenience, we have summarized these principles below:

1. **Accountability** – An organization is responsible for personal information under its control and shall designate an individual(s) who is accountable for the organization's compliance with established privacy principles.

   What you need to do

- Assign accountability for compliance with the ten (10) principles to a specific person or group of people in your company.

- Make available the identity and contact information of the person or group of people in your organization who are accountable for compliance with established privacy principles.

- Develop and then implement specific privacy polices and procedures.

- Use contracts and/or other measures to ensure that when third parties process personal information on your behalf, they maintain a level of privacy protection comparable to your own practices.

- Establish a complaint process to receive and respond to complaints and inquiries about your information management practices.

- Train your staff and ensure that they understand, and are capable of implementing, your privacy policies and practices.

2. **Identifying Purposes** – The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.

What you need to do

- Identify the legitimate purposes for collection personal information at or before the time you actually collect the information.

- Define what personal information is necessary to fulfill the purposes identified, taking into account both primary and secondary purposes (e.g., audit, marketing, etc.).

- Document your purposes so that your staff and the individuals to whom the information relates understand these purposes.

- When you want to use personal information already in your custody for a new purpose not identified at the time of the initial collection, seek the consent of the individual, unless the new purpose is required by law.

- Examine opportunities for using non-identifiable information (i.e., coded, anonymous, pseudonymous, or aggregated data) rather than identifiable individual information to meet your purposes.

3. **Consent** – The knowledge and informed consent of the individual are required for the collection, use or disclosure of personal information, except where exempted by law.

What you need to do

- Obtain consent for the collection, use and disclosure of personal information, at or before the time of collection, except where not appropriate (e.g., exchange of information with credit agency for a loan).

- Take into account the sensitivity of the personal information when determining what form of consent is appropriate for the circumstances (e.g., express or implied consent; opt-in or opt-out).

- Make a reasonable effort to advise the individual of the purposes for which the information will be used.

- Do not make the consent to the collection, use or disclosure of personal information for secondary purposes, such as marketing, a condition of the supply of your product or service.

- Do not deceive or mislead the individual in order to obtain consent.

- Inform individuals that they may withdraw consent at any time, and explain the implications of their withdrawal to them.

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.

What you need to do

- Limit both the type and amount of personal information you collect to only that which is necessary for your identified purposes.

- Collect personal information in a fair and lawful way, and do not deceive or mislead individuals.

- Do not collect personal information indiscriminately.

- Describe what type of personal information you collect and how it will be used and disclosed.

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 informed consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of those purposes.

What you need to do

- Use and disclose personal information in your control only for the purposes for which you collected it, unless you have obtained consent, or the use or disclosure are required by law.

- Document your use of personal information for any new purpose not initially communicated to the individual when receiving their consent.

- Retain information only as long as necessary to fulfill your identified purposes (have a policy of purging personal information from your databases).

- Retain personal information used to make a decision about an individual long enough to allow the individual to access that data and challenge its accuracy.

- Have procedures in place to govern the secure destruction of personal information.

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.

What you need to do

- Keep the personal information in your control only as accurate, complete and up-to-date as necessary for the identified purposes.

- Take into account the interests of the individual when determining how accurate, complete and up-to-date personal information in your custody needs to be.

- Ensure that personal information is sufficiently accurate to minimize the chances of inappropriate date being used when making decisions about individuals.

7. **Safeguards** – Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

What you need to do

- Implement security safeguards to protect personal information in your control against loss or theft, and unauthorized access, disclosure, copying, use or modification.

- Ensure that your security safeguards are appropriate and proportional to the sensitivity of the personal information in your custody.

- Protect all personal information in your control, regardless of its format.

- Make your staff aware of the importance of maintaining the confidentiality of personal information in your control.

- Dispose of or destroy personal information in a way that prevents unauthorized parties from gaining access to it.

8. **Openness** – An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

What you need to do

- Be open about your policies and practices with respect to the management of personal information.

- Make available details on the type of personal information you hold, how it is used and disclosed, and how individuals can request to know what personal information you hold about them.

- Enable individuals to obtain information about your policies and practices without an unreasonable effort.

- Make that information available in a format that is generally understandable.

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.

What you need to do

- Upon request, tell individuals if you have personal information about them and provide access to that data, except in limited circumstances.

- Tell individuals how their personal information is being used, and to whom it has been disclosed.

- Respond to an individual's request for access in a reasonable time, and at minimal, preferably no, cost.

- Provide the requested information to the individual in a format that is generally understandable, along with any explanation needed to facilitate the individual's understanding.

- Enable the individual to challenge the accuracy and completeness of personal information in your control and amend it as appropriate.

- Attach a statement of disagreement to records where you cannot agree to the requested amendment.

10. **Challenging Compliance** – An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual(s) accountable for the organization's compliance.

What you need to do

- Have procedures to receive and respond to complaints or inquiries about your handling of personal information.
- Explain your inquiry and complaint procedures to individuals.
- Investigate all complaints.
- Take appropriate measures to rectify the situation, if you find a complaint to be justified.
- Change your information management policies and practices, if necessary.

HOW CAN WE HELP?

If you are concerned about your organization's compliance with PIPEDA or are otherwise interested in this topic, **we can help in the following ways**:

1. Developing a privacy policy that is tailored to your organization.
2. Identifying those departments within your organization that collect personal information.
3. Holding a seminar on site at your organization where we explain the requirements of PIPEDA to departmental managers and train the managers sufficiently so that they can in turn train their staff.
4. Reviewing, assessing and modifying as necessary each relevant department's data collection practices to ensure that they, and any third parties that they may outsource to, are PIPEDA-compliant in respect of new and previously acquired personal information.
5. Creating ongoing operating procedures for the collection of data in compliance with PIPEDA including a complaints mechanism to deal effectively and efficiently with complaints under PIPEDA.
6. Reviewing, assessing and modifying (as applicable) any current employment agreements, consulting agreements, customer agreements and other supply chain agreements to ensure that they specifically permit the regular commercial activity undertaken by each department within your organization, including permission to disclose personal information in the context of due diligence in the event of a merger.
7. Developing a records retention and destruction policy that complies with PIPEDA.

CONCLUSION

Businesses must recognize the fact that lack of knowledge about privacy laws can threaten not only their public image but also their profits. Our team at Aylesworth can help you steer clear of the pitfalls of non-compliance with PIPEDA while maintaining good privacy practices for your business.

CONTACT INFORMATION

If you have questions or require further information, please contact our privacy law experts:

W. Eric Kay 416-777-4011 ekay@aylaw.com