

## **PIPEDA AND YOUR BUSINESS**

Owens, Wright LLP  
December 1, 2005

### **What is PIPEDA?**

In response to the concern for privacy in our society, the Canadian Government enacted the *Personal Information Protection and Electronic Documents Act* (PIPEDA). As of January 1, 2004 PIPEDA will apply to all provincially regulated organizations in provinces that do not have "substantially similar" privacy legislation. At present, Quebec is the only province who has such qualifying legislation.

PIPEDA creates an enforceable right of privacy for individuals with respect to the collection, use and disclosure of their personal information by the private sector. PIPEDA is groundbreaking legislation because it established Canada as the first country to implement private sector privacy rules.

### **Who is Bound by PIPEDA?**

All provincial organizations will be bound by PIPEDA as of January 1, 2004. An "organization" includes an association, a partnership, a person, a corporation and a trade union. PIPEDA applies retroactively, and therefore all personal information on past employees or customers from many years ago will also need to be protected.

### **What constitutes "personal" information?:**

Personal information is information about an identifiable individual that includes any factual or subjective data, recorded or not, in any form. For example, personal information might include:

- name, identification numbers, address, income, ethnic origin, blood type
- employee files, evaluations and disciplinary records
- driving records, credit and loan records, medical records
- documented disputes between consumer and merchant
- intention to acquire goods or services, or to change jobs
- opinions

### **The Substance of PIPEDA:**

There are three main provisions under PIPEDA:

#### **1. Handling the Collection and Management of Personal Information**

- You must state why the information is being collected at or before the time it is collected.
- You are only allowed to collect the information you need to fulfil your purpose.
- Personal information collected should be kept only as long as necessary; personal information that is no longer required should be destroyed, erased or made anonymous.

- All such information collected must be as accurate, complete, and up-to-date, although routine updates are not required under PIPEDA.
- After personal information is collected, it must be protected by security safeguards appropriate to the sensitivity level of the information. The more sensitive the information, the more protection it must receive. These safeguards must protect personal information from being lost or stolen, as well as any unauthorized access, disclosure, copying, use or modification. Methods of protection should include:
  - (a) Physical measures – e.g. locked cabinets, restricted access to offices
  - (b) Organizational measures– e.g. security clearances
  - (c) Technological measures – e.g. passwords, encryption
- All employees must be made aware of the importance of maintaining the confidentiality of personal information. Employees should receive a copy of all privacy policies and procedures and be trained in this area.

## **2. – Organizations Must Get Consent**

- You must get consent from individuals for the collection, use or disclosure of their information, unless the information is legally required such as a social insurance number for the statutory deduction of income at source.
- The information can then only be used for the purposes for which the individual gave consent; if the information needs to be used for a different purpose, you must obtain consent for the new use.
- Consent may be given in different ways. For example:
  - (a) an application form may be used to seek consent, collect information, and inform the individual of the use that will be made of the information;
  - (b) a checkoff box may be used to allow individuals to request that their names and addresses not be given to other organizations. Individuals who do not check the box are assumed to consent to the transfer of this information to third parties;
  - (c) consent may be given orally when information is collected over the telephone; or
  - (d) consent may be given at the time the individuals use a product or service.
- An individual may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice.

## **3. Individuals Right to Access Their Personal Information**

- You must be open about your privacy policies and practices and if asked, you must tell individuals about the existence, use, and disclosure of his or her information and give them access to that information.
- Information about your privacy policies can be made available in a variety of ways:
  - (a) through brochures available at your place of business;
  - (b) mailing information to customers;
  - (c) provide online access;
  - (d) establish a toll-free telephone number.
- If a customer or employee successfully challenges their personal information, you must amend or delete the information. If a challenge remains unresolved, this must be recorded and filed with the information by the organization.
- You must respond to a request for information within a reasonable period of time and at minimal or no cost to the individual. All information must also be provided in a manner that is easy to understand, for example, any abbreviations or codes must be explained.
- There are a few exceptions in which organizations may not be able to provide access to all the personal information it holds. Such situations include information that cannot be disclosed for legal, security, or commercial proprietary reasons, and information that is subject to solicitor-client privilege or litigation privilege.

### **On-Line Communications and PIPEDA:**

PIPEDA applies to all personal information whether it is in paper or electronic form. Therefore all electronic information management systems must comply with legislation as well. This affects the monitoring of employee's on-line communications. Before PIPEDA employers had the right to monitor their employee's email use and Internet viewing. Under PIPEDA however, monitoring such information will require employee consent. You may require such consent as a condition of employment, providing such a clause is reasonable. If you do not have any policies in this regard, adopt one. Provide copies of the policy to all existing employees notifying them that their "continued employment will be considered consent to this policy."

### **What is NOT covered by the PIPEDA?:**

- The collection, use or disclosure of personal information by federal government organizations listed under the *Privacy Act*;
- Provincial or territorial governments and their agents;
- The name, title, business address, or telephone number of an employee of an organization.

### **Four Steps to Compliance:**

There are four steps organizations must take in order to fulfil the legislative requirements:

#### **1. Analyze your handling of personal information**

- What personal information about customers and employees is collected?
- Why do you collect it?
- What personal information is used in carrying out business, for example, in sales, marketing, fundraising and customer relations?
- What personal information is obtained from, or disclosed to, affiliates or third parties?
- Where is such information kept?
- How is personal information secured?
- Who uses the information or has access to it?
- To whom is it disclosed?
- When is it disposed of and how is it disposed?

**2. Appoint an individual (or individuals) to be responsible for compliance**

You must designate someone within your organization to fill this role. The identity of the individual(s) must be made known upon request and should be identified in your privacy policy.

**3. Protect all personal information held by your organization or transferred to a third party for processing**

You need to ensure therefore that any information given to a third party by you is being adequately protected once it is in third party hands. This can be established through contractual agreement whereby the third party agrees to uphold all of your privacy policies and procedures, providing a comparable level of protection.

**4. Develop and implement personal information policies and practices.**

**Complaints:**

An individual may complain to the organization in question or to the Privacy Commissioner about any alleged breaches of the law. You must put procedures in place to deal with complaints or inquiries about their policies and practices relating to the handling of personal information. You must investigate all complaints. If a complaint is found to be justified you must take the appropriate measures, including, if necessary, amending your policies and practices.

**Enforcement:**

The Privacy Commissioner is responsible for overseeing and monitoring compliance with PIPEDA. The Commissioner has broad powers, including the power to:

- (a) audit or investigate an organization
- (b) summon individuals to give oral or written evidence under oath for an audit
- (c) enter the premises of an organization in order to assess compliance
- (d) converse in private with individuals on such premises
- (e) carry out any such on the premises any inquires he/she sees fit
- (f) examine or obtain copies of or extracts from records found on the premises

After an audit, the Commissioner will provide the audited organization with a report that contains the findings of the audit and any recommendations.

The Commissioner may also make public the information of the audit.

The Commissioner may report the commission of an offence against any law, provincial or federal to the appropriate authorities.

**Going To Court:**

If an individual is not satisfied with the Commissioner's report they may apply to the Federal Court of Canada.

The Commissioner can also apply to the Court on his or her own or on the complainant's behalf.

The Court may order an organization to change its practices and/or award damages to a complainant, including damages for humiliation suffered.

**Whistle-blowing:**

Any individual who believes that a person has contravened or intends to contravene PIPEDA can contact the Commissioner and request that their identity be kept confidential.

As an employer, you cannot dismiss, suspend, demote, discipline, harass or otherwise disadvantage an employee, or deny an employee a benefit of employment if the employee has disclosed information to the Commissioner or refuses to do anything because they believe it contravenes the act.

Any person who knowingly contravenes this provision or in any way interferes with an investigation is guilty of a summary offence and liable to a fine not exceeding \$10,000, or guilty of an indictable offence and liable to a fine not exceeding \$100,000.