

**DOING BUSINESS IN ONTARIO AND CANADA...**

**THE LEGAL OBLIGATION TO PROTECT PERSONAL INFORMATION IN CANADA**

*This is one a series of short articles in a series, **Doing Business in Ontario and in Canada**. The purpose of the series is to provide basic background information for non-Canadian companies wishing to establish a business presence in Canada, with a special focus on the Province of Ontario.*

Since January 1, 2004, the *Personal Information Protection and Electronic Documents Act* (PIPEDA) has applied to all organizations that carry on commercial enterprises in Canada. This article summarizes the basic compliance obligations of PIPEDA, identifies some common compliance issues, and proposes some suggestions which businesses need to consider to be compliant with the Act.

Experience to date since the enactment of the legislation suggests that, with some careful planning and education/awareness programmes within their organizations, businesses are able to genuinely comply with the spirit and intent of the legislation.

**Why comply with PIPEDA?**

Individuals have become increasingly concerned about the unauthorized and indiscriminate collection, use and/or dissemination of personal information. Greater public awareness of fraud by “identity theft” has also prompted more attention by individuals to their privacy rights. Therefore, protecting personal information is good business.

Non-compliance with PIPEDA may have serious consequences in the form of directives from the Federal Privacy Commissioner and court orders issued by the Federal Court to comply with PIPEDA, as well as awards of damages (including damages for humiliation). The Federal Privacy Commissioner has the power to conduct an audit of an organization’s compliance, for which purpose the Commissioner has broad powers to summon witnesses, take affidavits, require document production and inspection. The costs to be incurred by an organization subject to an audit are likely to be substantial.

At the outset, we offer two PIPEDA warnings for those who may be establishing new businesses in Canada. First, it is illegal (subject to some exceptions) to withhold goods or services because a person refuses to give his or her consent to the collection, use or disclosure of personal information. Second, in response to a request from someone for their personal information (see below, Privacy Principle No. 9), it is an offence to simply delete the information.

**PIPEDA’s Scope.**

PIPEDA defines “personal information” (with great brevity) as “information about an identifiable individual”. Such personal information includes (and by no means is limited to) information of an identifiable individual such as marital status, age, weight, religion, gender, income, favorite beverage, SIN number, travel history, credit history, make of car, golf handicap, spouse’s name, number of children and so on.

The only exclusions to this expansive definitions are a person's name, title, and work address and telephone number in the context of that person's employment. So information relating to John Doe, Associate Lawyer, at Morrison Brown Sosnovitch LLP is not personal information if the record relates to Morrison Brown Sosnovitch LLP. However the same information (name, job title, work address and work telephone number) would be personal information concerning John Doe in the file of a credit reporting agency or a golf club to which John Doe belongs.

PIPEDA applies to personal information about an identifiable individual. Until case law resolves the ambiguity, organizations should treat information relating to 'incorporated individuals' and perhaps small incorporated businesses as being identifiable to the individual who has incorporated or the principals of the small incorporated business. For example, credit information relating to "Nancy Drew Detective Agency Inc." is probably identifiable also as credit information about Nancy Drew as an individual, and should be treated as such.

The scope of PIPEDA is also limited to a "commercial activity", which is broadly defined as "any particular transaction, act or conduct or any regular course of conduct that is of a commercial character". The non-commercial collection, use and disclosure of personal information is not covered by PIPEDA. Thus the maintenance of an address book (including an electronic address book) for personal use is not covered, but the transfer of information in the address book in a commercial transaction is within the mandate of PIPEDA and would require, for example, the consent to disclosure of the individuals to whom the information relates.

PIPEDA also applies to "organizations". This obviously includes companies, but as well includes a partnership, a person, a trade union and an association. It also applies to organizations outside Canada which wish to carry on business in Canada. Since PIPEDA is the most comprehensive privacy legislation in North America and is quite different from the sectoral and self regulation approach in the US, US enterprises are likely to find compliance with PIPEDA a new experience. The burden is likely to be much less for European business because PIPEDA in many ways is founded upon models which originated in, and are in common use, in the European Union.

### **Provincial Exemptions.**

There are very few exemptions from PIPEDA's applications, but one of the key exemptions is the ability of Parliament to exempt from PIPEDA organizations carrying on commercial activity within a province which has enacted substantially similar legislation. To date, Ontario has not enacted such legislation (except in the area of health information). The Province did release draft legislation in 2000 for comment, but no bill was ever tabled in the Ontario legislature, and it is understood that a bill is unlikely in the foreseeable future. Even if Ontario enacted substantially similar legislation, PIPEDA would continue to apply to interprovincial commercial activities, as well as to federally regulated industries within the province (such as banks). Therefore, business should hope that all provincial legislation, if the provinces opt to enact their own statutes, will be substantially identical so that businesses do not have to conform to a differing patchwork quilt of legislation across the country.

## **THE TEN PRINCIPLES OF PRIVACY PROTECTION**

The main privacy obligations of PIPEDA are succinctly stated in section 5 which states (subject to certain exceptions), that "...every organization shall comply with the obligations set out in Schedule 1".

Attached is a short Summary of the 10 privacy principles set out in Schedule 1 to PIPEDA. These principles are derived from the Canadian Standards Association "Model Code for the Protection of Personal Information". Although the CSA's Model Code itself does not have the force of law, PIPEDA effectively elevates the code to this status. These 10 principles effectively set the standard by which all

privacy policies are judged, and a thorough understanding of the principles is necessary on the part of the Privacy Officers (which every organization is required to appoint as set out in the first principle, entitled “Accountability”).

These principles should be reviewed and considered in the context of the four most significant activities relating to the handling of personal information, namely:

1. the collection of personal information;
2. the use of personal information;
3. the retention and storage of personal information; and
4. the disclosure of personal information.

### **Becoming Compliant – What to do**

Any new business seeking to establish itself in Canada needs to undertake any analysis of its information needs and design its business systems to ensure PIPEDA compliance without undue interference to efficient business operations. Following is an outline of the basic steps to creating an effective, efficient and legal framework for managing personal information.

1. Assess your organization’s information needs for personal information.
  - What personal information is the business likely to acquire? Consider this in the context of information relating to customers, prospective customers, suppliers, contractors and employees.
  - What information does it reasonably need? For what purposes? What information will not have to be retained?
  - What is the best way to collect information and obtain the individual’s consent to its collection, use, retention and disclosure?
2. *Appoint a Privacy Officer* to oversee implementation and to fulfill the role of ensuring compliance. Be sure this person is provided with relevant materials training and sufficient resources.
3. *Develop a plan for obtaining consents* for all personal information to be collected and which needs to retain for its identified purposes. Include in the plan a strategy for using the process of obtaining consent for also giving notice regarding the use and disclosure of personal information and to confirm the accuracy of the personal information already held.
4. *Develop a plan for protecting personal information*, giving consideration to physical location, responsibility and technology restrictions, such as passwords. The plan must protect against unauthorized access, disclosure, copying, use as well as theft, and unauthorized destruction or modifications.
5. *Ensure your plan facilitates retrieval* of personal information, efficiently and accurately. First and foremost, in order to have the legal right to retain personal information, your organization must have a reasonable and identified need for it, so make sure it is appropriately accessible by the right people for the right purposes. Secondly, the Access Principle requires that organizations

be able to produce the information upon enquiry of an individual, including information as to its use and disclosure.

6. *Assign accountabilities.* Provide or arrange for appropriate training and instruction, and create awareness by all persons who have or may have access to personal information.
7. *Design a fair complaint procedure.*
8. *Put the plan in writing.* PIPEDA requires your policies to be in writing and to be clear, understandable and readily available.

There may be more than one plan for different classes of information. For example, a good plan may be quite different for information relating customers as opposed to employees because the information will likely be retained for different purposes, will likely be stored differently, and persons with authorized access may differ.

**For more information on personal information practices, contact Wes Brown at Morrison Brown Sosnovitch LLP, 1 Toronto Street, Suite 910, Toronto, ON M5C 2V6, phone (416) 368-0600 fax (416) 368-6068 email: [wbrown@businesslawyers.com](mailto:wbrown@businesslawyers.com).**

Visit our website at [www.businesslawyers.com](http://www.businesslawyers.com)

© Morrison Brown Sosnovitch LLP, 2008 All rights reserved.

## **THE TEN PRIVACY PRINCIPLES**

### **1. Accountability**

An organization must designate an individual to be accountable for the organization's compliance with the Act. This individual, whose identity must be made known upon request, is responsible to (i) implement procedures to protect personal information; (ii) to retrieve and respond to complaints and inquiries; (iii) training and communication in the organization relating to privacy; and (iv) the explanation of the organization's policies and procedures.

### **2. Identifying Purposes**

An organization must document the purposes for which personal information is collected. If personal information is to be used for a previously undisclosed purpose, the organization must inform and obtain the individual's consent before the information is used for that purpose, unless the use or disclosure is required by law.

### **3. Consent**

An individual's consent is required for the collection, use or disclosure of personal information except where obtaining such consent is inappropriate. When obtaining consent, an organization should make it very clear what information is being collected and how such information will be used. The way in which an organization seeks consent may vary depending on the circumstances. Implied consent may be sufficient when dealing with general information that is not of a personal nature but explicit consent should be obtained when dealing with personal or sensitive information.

### **4. Limiting Collection**

The collection of personal information must be limited to that which is necessary for the purposes of the organization. Information should be collected through fair and lawful means and individuals should not be in any way misled or 'duped' into providing personal information.

### **5. Limiting Use, Disclosure and Retention**

Personal information must not be used for any purpose other than those that the individual consented to or that is required by law. Information should not be retained longer than necessary and should be destroyed, erased or made anonymous when it is no longer required to fulfill the identified purpose. An organization should develop guidelines and implement procedures to govern the destruction of information.

### **6. Accuracy**

Personal information must be as accurate, complete and up to date as is necessary for the purpose for which it is used. An organization must not routinely update personal information unless such updating is necessary for the purpose for which the information is used.

### **7. Safeguards**

Safeguards should be employed to protect the information against loss, theft or unauthorized access, disclosure, copying, use or modification. Methods of protection should include physical measures, such as locking filing cabinets, organizational measures, such as security clearances, and technological measures, such as the use of passwords and encryption.

## **8. Openness**

An organization should be open about its policies and practices with respect to the management of personal information. This means that the organization must make available information about its policies and practices. Such information should include the name and address of the person accountable for the organization's privacy policies and practices, the means of gaining access to information held by the organization, a description of the information held by the organization and what information is made available to related organizations, such as subsidiaries.

## **9. Individual Access**

An individual must, within a reasonable amount of time, be informed of the existence, use and disclosure of his or her personal information and must be given access to that information. In providing an account of third parties to which personal information has been disclosed, an organization should be as specific as possible. If an individual demonstrates the inaccuracy or incompleteness of personal information, the organization must amend such information as required.

## **10. Challenging Compliance**

An individual should be able to address an issue relating to an organization's compliance with the above principles to the organization's privacy officer. An organization should put into place procedures to receive and respond to complaints. All complaints must be investigated and an organization must take appropriate measures to remedy problems.