Thompson Law Professional Corporation
Barrister & Solicitor, Notory Public, Registered Trade Mark Agent, Paralegal

Privacy: A Primer for Small Business Owners

The contents of this Memorandum relate, generally, to the Privacy law in the Province of Ontario, Canada. It is not intended to be relied upon to provide legal advice for any particular set of circumstances, and liability for any such use is disclaimed. Always consult a lawyer qualified to practice law in the Province of Ontario, Canada, for legal advice with respect to Privacy law generally and specifically with respect to the creation of a Privacy Policy for your business.

What is Privacy?

The Office of the Privacy Commissioner of Canada defines the right to privacy as: "The right to control access to one's person and information about oneself."

Privacy is a fundamental right and is protected by several laws. Apart from federal laws, supranational organizations such as the United Nations, the Organization for Economic Cooperation and Development and the European Union have established laws respecting a individual's privacy. One must be aware of the scope of the legislation to determine your rights and obligations.

What is a Privacy Policy?

A Privacy Policy is a collection of guidelines a company or organization uses to manage the personal information collected about people. The policy reflects the purposes for the collection of personal information and the type of information which is collected. Additionally the policy includes several other aspects such as a description of the uses of personal information, circumstances of disclosure of personal information and processes for examination and correction of personal information. It may also describe the extent to which people have control over how their information will be collected, disclosed or otherwise used.

If the company makes use of the Internet then a Privacy Policy published on the website or homepage should depict the management of personal information of visitors to the site.

The visitor to the website should be informed about the collection, use and disclosure of his personal information, including:

- other Internet related aspects, such as the usage of cookies;
- links to other websites; and
- server logs.

Vcard Info

Thompson Law Professional Corporation
511 Welham Road, Unit 1
P.O. Box 696
Barrie, Ontario L4M 4Y5

Telephone: (705) 727-1124
Facsimile: (705) 722-8246
Email: info@iobject.ca

Website

WHAT IS "PERSONAL INFORMATION"?

Personal information is any factual or subjective information, recorded or not, about an identifiable individual. Personal information includes:

- Personal and physical characteristics such as name, age, weight, height, ethnic origin;
- Personal Identification numbers, including Social Insurance Numbers;
- Medical History and Records including, for example, blood type;
- Economic status including: Income, Credit and Loan records, consumer/commercial dispute records, employee files including disciplinary action and evaluations and Social Status;
- Generally any recorded opinion and comments concerning an individual.

Personal information does not include:

- job title;
- telephone number or address; and
- anything that might appear on a business card or can be found through publicly available information such as the yellow pages, the telephone book or the Internet.

Note that this definition of "personal information" is current to Canadian Law as at June 1, 2005. If your business or organization deals with other countries, there might be differences in the definition due to other laws.

DO I NEED A PRIVACY POLICY?

Privacy is a fundamental right. Two federal laws protect Canadians: the Privacy Act and the Personal Information Protection and Electronic Documents Act (PIPEDA). The Privacy Act imposes obligations on government departments and agencies to respect the privacy rights of Canadians by placing limits on the collection, use and disclosure of personal information. The Privacy Act gives Canadians the right to access and correct personal information about them held by federal government organizations.

PIPEDA covers the collection, use and disclosure of personal information in the course of any commercial activity within the provinces, including provincially regulated organizations. PIPEDA impacts the federally regulated sector in the course of commercial activities and all businesses and organizations engaged in commercial activity in Yukon, the Northwest Territories and Nunavut, as well as, information sold across territorial and provincial boundaries. Also, the personal health information collected, used or disclosed by these organizations is protected.

Even if a Privacy Policy were not required by law, it is strongly recommended to develop a Privacy Policy for your business. Protecting the privacy of the public is sensible business.

Specifically, trust is very important in all kind of relationships, especially to developing positive public relations. Further, it is a competitive advantage over other businesses who do not explain their procedures of dealing with personal information.

Hence, the Privacy Policy will help you to avoid legal actions, to avoid negative publicity and to maintain a good relationship with your customers, clients and employees.

How Does The Personal Information Protection and Electronic Documents Act Protect Personal Information?

The law requires organizations to:

- obtain a person's consent when collecting, using or disclosing personal information;
- supply a person with a product or a service even if they are refusing to consent to the collection, use or disclosure of their personal information unless the information is essential to the transaction;
- collect information by fair and lawful means;
- provide personal information policies that are clear, understandable and readily available; and
- destroy, erase or make anonymous personal information about their customers that are no longer needed in order to fulfill the purpose for which they were collected.

There are some exceptions to these requirements. For example, an organization may not need to obtain a person's consent if collecting the information is required by law. During an investigation, an enforcement agency is not required to obtain consent because obtaining consent might compromise the accuracy of the information.

What is NOT Covered by PIPEDA?

PIPEDA does not impact:

- The Collection, use or disclosure of personal information by federal government organizations listed in the *Privacy Act*;
- Provincial or territorial governments and their agents;
- An employee's name, title, business address or telephone number;
- An individual's collection, use or disclosure of personal information strictly for personal purposes (personal greeting card list); and
- The collection, use or disclosure of personal information solely for journalistic, artistic or literary purposes.

What Must Be Included in a Privacy Policy?

PIPEDA was established on the basis of the Canadian Standards Association (CSA) Model Code for the Protection of personal information. It contains 10 principles which must be adopted by your organization. It is recommended that you include these principles in a Privacy Policy in order to show in detail how your organization complies with the law.

Here is a summary of the principles required by your organization to implement the law and what kind of information and details should be part of the policy:

1. Accountability

   Your organization recognizes its responsibility for the management of personal information according to the 10 principles. You must designate an individual who will be accountable for compliance and developing procedures and policies.

2. Identify the purpose

   Your organization must demonstrate the purposes for the collection of personal information. The reasons for collection and use must be obvious for the public before or at the time of collection. Attention should be drawn to the consent and the reason for collection using a bold font or checkbox for example.

3. Obtain Consent

   Your organization must proclaim that it obtains the consent before or at the time of collection, use or disclosure of personal information. More importantly, your organization does not try to obtain consent by deceiving the public.

4. Limiting Collection

   Your organization shows a commitment to limiting collection of personal information from several points of view. You are required to supply customers with products and services even when they only give consent to collect the information needed to complete your business. Your organization does not deceive or mislead individuals about the reasons for the collection of information.

5. Limited Use, Disclosure and Retention

   Use, disclosure and retention of personal information must be limited. Except where it is required by law, personal information should not be used, disclosed and retained without the consent of the person.

6. Accuracy

   Your organization should keep personal information as accurate, complete and up-to-date as necessary for the identified purposes for which it was collected.

7. Safeguards

   Your organization should demonstrate that personal information is safeguarded appropriately given the sensitivity of the information. Personal data must be protected from unauthorized access, disclosure, copying, use or modification. This may mean locking up files or limiting access to databases by password.

8. Openness

   Your organization must create an understandable Privacy Policy for the public. Making easily available the policies and practices of your company is a major part of being open.

9. Individual Access

   Your organization must allow individuals access to their personal information held by your organization. Moreover, an individual must also have the ability to correct inaccurate or incomplete information.

10. Challenging Compliance

    Your organization must demonstrate that you have developed a simple and easily accessible complaint procedure. You must inform the complaining individuals about the steps taken by the company. Finally, you must correct procedures and policies as required.

Retention of Information

You must inform a person how long their personal information will be retained. Further you must inform a person about procedures after it is no longer necessary to retain their information. You should detail how you destroy the files or erase the information.

COMPLIANCE

The process of compliance is time consuming. First, analyze all of the processes in your organization dealing with personal information. Then, create a policy according to law. Eventually transfer the policy into the day-to-day operations of your organization. Procedures related to personal information may be adjusted. Staff must be trained. Finally, persons accountable and in charge for answering requests should be selected, so that your company meets all of the requirements of law.

WHAT ARE THE RISKS OF NON-COMPLIANCE?

A failure to comply can expose your firm to a number of costly, time-consuming and potentially embarrassing circumstances. PIPEDA makes the federal Privacy Commissioner responsible for promotion and for ensuring compliance with the Act. The Commissioner has five main ways of ensuring that organizations subject to the Act adhere to its principles:

- investigating complaints;
- mediating and conciliating complaints;
- auditing personal information management practices;
- publicly reporting abuses; and/or,
- seeking remedies in court.

An individual may complain to the organization in question or to the Privacy Commissioner about any alleged breaches of the law. A person who believes that anyone has contravened or intends to contravene, sections 5 to 10 of PIPEDA, may notify the Privacy Commissioner. The person may ask that his or her identity be kept confidential. Once the Privacy Commissioner has given his assurance, the Commissioner is bound to protect the person's identity.

The Privacy Commissioner may also initiate a complaint. A complaint will prompt an investigation and the preparation of a report.

After receiving the Commissioner's investigative report, a complainant may, under certain circumstances, apply to the Federal Court for a hearing. The Privacy Commissioner may also apply to the Court on his own or on the complainant's behalf. The Court may order an organization to change its practices. Of course, legal fees to defend could be very large and the Court may award costs to the Privacy Commissioner; altogether an expensive outcome.

The Privacy Commissioner may, on reasonable grounds, audit the personal information management practices of an organization.

An audit or complaint that results in a public report about breaches of compliance at your organization could be damaging to your reputation.

It is an offence to:

- destroy personal information that an individual has requested;
- retaliate against an employee who has complained to the Privacy Commissioner or who refuses to contravene Sections 5 to 10 of PIPEDA; and
- obstruct a complaint investigation or an audit by the Privacy Commissioner or his delegate.

A person is liable to a fine of up to $ 10,000 on summary conviction or up to $ 100,000 for an indictable offence.

WHAT DO I HAVE TO NOTE ABOUT THE STYLE IN A PRIVACY POLICY?

Part of the openness principle is to be clear and understandable. The Privacy Policy must be readable. For example, a yellow font on a white background is quite difficult to read, as is brown print on a tan background. For a clear example of the wrong thing to do, check out the fine print on some legal documents that is so small as to be virtually illegible to the naked eye.

A Privacy Policy must be understandable and relatively simple to comprehend. Avoiding long sentence structures is helpful.

SHOULD I CONSULT A LAWYER TO DRAFT A PRIVACY POLICY OR CAN I CREATE IT INTERNALLY?

While it is not necessary to obtain the assistance of a lawyer in preparing your Privacy Policy, it is recommended. Every organization is allowed to create the policy on their own. There are some do-it-yourself-kits available.

Nevertheless, you should be aware of the risks involved in preparing the policy on your own:

- Due to a lack of experience, the policy might not cover all of the relevant issues;
- A complaint may be made with the attendant costs;
- Negative publicity and negative employee moral are a likely result from the mismanagement of personal information due to a poor Privacy Policy; and
- Ensuring inclusion of all the relevant details for your organization is time consuming.

Advantages of consulting a lawyer are:

- The Privacy Policy will be tailored to your organization and profession;
- The Privacy Policy will cover all relevant issues and assist to prevent your organization from being confronted with legal action;
- The Privacy Policy will maintain a good relationship with the public; and
- The Privacy Policy has more credibility if it is linked to a third-party advocate who can verify your commitment to protect your customers.

HOW DOES THE LEGISLATION IMPACT ON INTERNATIONAL TRANSACTIONS?

Beginning January 1, 2004, PIPEDA has applied to all collection, use or disclosure of personal information that occurs in the course of commercial activities of Canadian organizations, including across an international border. Hence, organizations will be required to apply the principles of PIPEDA to these transactions also.

Certain countries or regions have implemented privacy laws that impose privacy protection rules on international trade. For example, the European Union Data Protection Directive, which applies to all European Union (EU) member countries, allows only the transfer of personal data to countries that provide an adequate level of privacy protection.

Directive 95/46/EG, a decision of the European Commission on December 20, 2001, has recognized PIPEDA as providing adequate protection for the transfer of personal information from the EU to Canada. It allows the flow of personal information between the EU and Canada without additional guaranties.

Is It Possible to Outsource the Processing of Personal Information to an Organization Located in a Country With a Less Strict Privacy Laws?

PIPEDA states that organizations are responsible for personal information that has been transferred to a third party for processing. According to Principle 1 in the Act, the organization is accountable for using contractual or other means to ensure that a comparable level of privacy protection will be provided while the information is being processed by the third party.