Personal Information Protection Policy for Small and Medium-Size Businesses

Why does a small business need a policy?

Alberta's *Personal Information Protection Act*, which came into force on January 1, 2004, requires every organization to designate an individual to be responsible for the organization's compliance with the Act. The Act also requires organizations to develop and follow reasonable personal information protection policies and practices to enable them to comply with the Act.

What are the requirements of a personal information protection policy?

A policy must explain how an organization will put the Act into effect with respect to the personal information that is collected, used and disclosed by that particular organization. The policy should address matters that arise regularly in the course of the organization's business.

It is important to have policies that comply with the Act and that are reasonable for your organization to implement, since your clients will rely on them.

The last few years have seen increasing consumer demand for the sensitive handling of personal information by all businesses. Developing a personal information protection policy and adhering to good privacy practices is an effective way of anticipating or responding to questions. A policy that promotes privacy can also be used as a marketing tool, as well as a support for training and compliance within the organization.

Your personal information protection policy should be brought to the attention of your clients. It can be communicated through a brochure or on your website, for example, and must be available for inspection on request.

If your organization uses service providers outside of Canada, to collect, use, disclose, or store personal information, your policy must identify the countries in which the collection, use, disclosure or storage is occurring, or may occur, and explain the purposes for which the service provider is authorized to collect, use, disclose personal information for or on behalf of your organization.

How does my business develop a policy?

The sample policy provided here is a policy for the protection of the personal information of clients. It does not address the protection of personal employee information. It is offered as a starting point for explaining your own practices in a way that is meaningful to your clientele. The words and phrases highlighted in green should be modified to suit your business. The green arrowed boxes offer suggestions. The blue boxes offer additional information and tips. You can omit any paragraphs that are not applicable to your own organization.

The most important point to remember is, *Say what you mean and do what you say*.

This guide to developing a privacy policy was prepared by Access and Privacy, Service Alberta to assist organizations in implementing the *Personal Information Protection Act*. It is not intended as, nor is it a substitute for, legal advice. The guidance provided here is not binding on the Office of the Information and Privacy Commissioner of Alberta. For further information, visit Access and Privacy's website at pipa.alberta.ca or call 780-644-PIPA (7472). Call toll free in Alberta by first dialing 310-0000.

Name of your Organization

Personal Information Protection Policy

Name of your organization is committed to safeguarding the personal information entrusted to us by our clients. We manage your personal information in accordance with Alberta's *Personal Information Protection Act* and other applicable laws. This policy outlines the principles and practices we follow in protecting your personal information.

This policy applies to Name of your organization and its subsidiaries, Names of subsidiaries. The policy also applies to any person providing services on our behalf.

A copy of this policy is provided to any client on request.

What is personal information?

Personal information means information about an identifiable individual. This includes an individual's name, home address and phone number, age, sex, marital or family status, an identifying number, financial information, educational history, etc.

What personal information do we collect?

We collect only the personal information that we need for the purposes of providing services to our clients, including personal information needed to:

- open and manage an account
- deliver requested products and services
- enrol a client in a program
- guarantee a travel or hotel reservation
- process a magazine subscription
- send out association membership information
- assess suitability for tenancy
- provide warranties for products and services
- contact clients about appointments
- follow up with clients to determine satisfaction with products and services
- notify clients of upcoming events of interest
- administer our loyalty program
- grant credit
- meet regulatory requirements
- other (specify)

We normally collect client information directly from our clients. We may collect your information from other persons with your consent or as authorized by law.

We inform our clients, before or at the time of collecting personal information, of the purposes for which we are collecting the information. However, we don't provide this notification when a client volunteers information for an obvious purpose (for example, producing a credit card for an in-store purchase when the information will be used only to process the payment).

Choose the word(s) most appropriate for your clientele. Do they think of themselves as "clients," or as customers, members, students, tenants, patrons, or subscribers?

Your policy may be posted in your premises, distributed with statements or promotional material, posted on your web site or some combination of these methods. A privacy policy can be an effective marketing tool.

Include some examples of personal information that your organization collects.

These are only examples. Your policy should list the purposes for which your organization collects personal information.

A "model" policy might specify what personal information is collected for each purpose (e.g. what information your organization collects to perform a credit check).

Choose an example that fits your organization. When are your clients likely to volunteer personal information?

Use of Service Providers outside Canada

Our service providers in the U.S.A. collect, use or disclose your personal information for the following purposes:

- open and manage an account
- deliver requested products and services
- enrol a client in a program [specify program]
- guarantee a travel or hotel reservation
- process a magazine subscription
- send out association membership information
- provide warranties for products and services
- follow up with clients to determine satisfaction with products and services
- notify clients of upcoming events of interest
- administer our loyalty program
- grant credit
- other (specify)

These are only examples. Your policy should identify the countries in which the collection, use, disclosure or storage is occurring and the purposes for which the service provider collects, uses, or discloses personal information on your behalf. If you use service providers in different countries for different services, specify which services are fulfilled in each country.

Consent

We ask for consent to collect, use or disclose client personal information, except in specific circumstances where collection, use or disclosure without consent is authorized or required by law. We may assume your consent in cases where you volunteer information for an obvious purpose.

In cases where we collected personal information before January 1, 2004, we assume your consent to our use and, where applicable, disclosure for the purpose for which the information was collected.

We ask for your express consent for some purposes and may not be able to provide certain services if you are unwilling to provide consent to the collection, use or disclosure of certain personal information. Where express consent is needed, we will normally ask clients to provide their consent orally (in person, by telephone), in writing (by signing a consent form, by checking a box on a form, or electronically (by clicking a button).

In cases that do not involve sensitive personal information, we may rely on "opt-out" consent. For example, we may disclose your contact information to other organizations that we believe may be of interest to you, unless you request that we do not disclose your information. You can do this by checking the appropriate box on our application form or by telephoning our local number/toll-free number.

A client may withdraw consent to the use and disclosure of personal information at any time, unless the personal information is necessary for us to fulfil our legal obligations. We will respect your decision, but we may not be able to provide you with certain products and services if we do not have the necessary personal information.

We may collect, use or disclose client personal information without consent only as authorized by law. For example, we may not request consent when the collection, use or disclosure is reasonable for an investigation or legal proceeding, to collect a debt owed to our organization, in an emergency that threatens life, health or safety, or when the personal information is from a public telephone directory.

You do not need to obtain consent to use personal information collected before 2004, but it is a good practice to seek consent when you update that information.

Describe how you normally obtain consent. It is helpful to clients if you can specify the form of consent you use in different circumstances.

Include this paragraph only if you use opt-out consent. Describe the actual method you use.

The complete list of circumstances in which personal information may be collected, used or disclosed is listed in sections 11, 14 and 17 of PIPA (*Guide*, pp. 27-33). Choose examples relevant to your organization.

How do we use and disclose personal information?

We use and disclose client personal information only for the purposes for which the information was collected, except as authorized by law. For example, we may use client contact information to deliver goods. The law also allows us to use that contact information for the purpose of collecting a debt owed to our organization, should that be necessary.

If we wish to use or disclose your personal information for any new business purpose, we will ask for your consent.

How do we safeguard personal information?

We make every reasonable effort to ensure that client information is accurate and complete. We rely on our clients to notify us if there is a change to their personal information that may affect their relationship with our organization. If you are aware of an error in our information about you, please let us know and we will correct it on request wherever possible.

In some cases we may ask for a written request for correction.

We protect client personal information in a manner appropriate for the sensitivity of the information. We make every reasonable effort to prevent any loss, misuse, disclosure or modification of personal information, as well as any unauthorized access to personal information.

We will notify the Office of the Information and Privacy Commissioner of Alberta, without delay, of a security breach affecting personal information if it creates a real risk of significant harm to individuals.

We retain client personal information only as long as is reasonable to fulfil the purposes for which the information was collected or for legal or business purposes.

We render client personal information non-identifying, or destroy records containing personal information once the information is no longer needed.

We use appropriate security measures when destroying client personal information, including shredding paper records and permanently deleting electronic records.

A model policy would list some examples of physical, technological and administrative measures used to protect personal information, such as IT network security and restrictions based on the "need to know" on employee access to personal information.

Remember you will be held to what you say in your policy, so your policy must reflect your actual practices.

Access to records containing personal information

Clients of Name of organization have a right of access to their own personal information in a record that is in our custody or under our control, subject to some exceptions. For example, organizations are required under the *Personal Information Protection Act* to refuse to provide access to information that would reveal personal information about another individual. Organizations are authorized under the Act to refuse access to personal information if disclosure would reveal confidential business information. Access may also be refused if the information is privileged or contained in mediation records.

The complete list of exceptions to access appears in section 24 of PIPA (*Guide*, pp.41-2). Choose examples that are relevant to your organization.

If we refuse a request in whole or in part, we will provide the reasons for the refusal. In some cases where exceptions to access apply, we may withhold that information and provide you with the remainder of the record.

You may make a request for access to your personal information by writing to Name or position title of individual in your organization designated to ensure compliance with PIPA. You must provide sufficient information in your request to allow us to identify the information you are seeking.

PIPA requires every organization to designate an individual to be responsible for compliance with the Act.

You may also request information about our use of your personal information and any disclosure of that information to persons outside our organization. For personal information collected before January 2004, if we do not have a record of disclosures, we will provide information about any disclosure of your information that is likely to have occurred.

You may also request a correction of an error or omission in your personal information.

We will respond to your request within 45 calendar days, unless an extension is granted. We may charge a reasonable fee to provide information, but not to make a correction. We will advise you of any fees that may apply before beginning to process your request.

An organization that receives a lot of requests may find it helpful to develop a schedule of fees.

Questions and complaints

If you have a question or concern about any collection, use or disclosure of personal information by Name of organization, or about a request for access to your own personal information, please contact Name or position title of individual in your organization designated to ensure compliance with PIPA in the first instance:

Name or position title of designated individual
Name of organization
Contact information

If you are not satisfied with the response you receive, you should contact the Information and Privacy Commissioner of Alberta:

Office of the Information and Privacy Commissioner of Alberta
Suite 2460, 801 - 6 Avenue, SW
Calgary, Alberta T2P 3W2
Phone: 403-297-2728 Toll Free: 1-888-878-4044
E-mail: generalinfo@oipc.ab.ca Website: www.oipc.ab.ca