



Office of the Information  
and Privacy Commissioner

Suite 2460, 801 – 6th Ave. SW  
Calgary, Alberta  
T2P 3W2  
Phone: (403) 297-2728  
Fax: (403) 297-2711  
Toll Free: 1-888-878-4044  
Web: [www.oipc.ab.ca](http://www.oipc.ab.ca)  
Email: [generalinfo@oipc.ab.ca](mailto:generalinfo@oipc.ab.ca)

***Personal Information Protection Act (PIPA)***  
**PIPA ADVISORY #1**  
**IMPLEMENTING CONSENT REQUIREMENTS FOR CUSTOMERS**

This document was prepared to help organizations implement the *Personal Information Protection Act* which came into effect on January 1, 2004. This document is an administrative tool intended to assist in understanding the Act. It is not intended as, nor is it a substitute for, legal advice. For the exact wording and interpretation of PIPA, please read the Act in its entirety. This Advisory is not binding on the Office of the Information and Privacy Commissioner of Alberta.

**Contents**

[Introduction](#)  
[What is Personal Information?](#)  
[Limitations on Application of The Act](#)  
[The Act Requires Reasonableness](#)  
[Understanding Consent Requirements](#)  
[Express Consent](#)  
[Opt-Out Consent](#)  
[Implied Consent](#)  
[Information Collected Before January 1, 2004](#)  
[Consent Must Relate to a Specific Purpose](#)  
[Consider the Sensitivity of Information](#)  
[Disclosure](#)  
[Collection, Use and Disclosure Without Consent](#)  
[Variation or Withdrawal of Consent](#)  
[Notification and Consent Checklist](#)  
[Other Resources](#)

**Introduction**

The *Personal Information Protection Act* (PIPA or the “Act”) sets out the requirements for how private sector organizations collect, use, disclose and protect personal information. The Act recognizes the right of an individual to have his or her personal information protected, and the need of organizations to collect, use or disclose personal information for reasonable purposes.

Except where the Act says otherwise, organizations must get consent to:

- collect personal information,
- collect personal information from someone who is not the individual,
- use personal information, or
- disclose personal information.

**NOTE:** Personal employee information receives special treatment under the Act. For more information, see sections 15, 18 and 21 of the Act.

**What is Personal Information?** Personal information is any information, recorded or not, for an identifiable individual. It includes, for example:

- name, home address, age, weight, height, gender
- employment or financial history
- ID numbers, place of birth, ethnic origin
- opinions, evaluations, or comments about an individual

The Act does not apply where it is not possible to identify a specific individual from the information.

**Example:** An organization could gather information from thousands of customers about what they buy, whether price is important, their gender, etc., as long as the data did not identify individuals.

**TIP:** Organizations should be careful when trying to determine if information is anonymous as they may not be aware of how the information could be matched to an identifiable individual (for example, by combining it with information from more than one source).

**Limitations on Application of The Act**

Not all personal information is covered by the Act. For example, the Act does not apply to business contact information where it is collected, used or disclosed solely for the purpose of contacting an individual in a business capacity. Business contact information is defined in the Act to mean an individual's name,

position name or title, business telephone number or address, e-mail, fax number, and other similar business information.

Consent is required when business contact information is collected, used or disclosed for any other reason, unless the Act provides an exception.

Other examples of personal information which are not governed by PIPA are listed in Section 4(3) of the Act and include personal information:

- in the custody or control of public bodies or governed by the *Freedom of Information and Protection of Privacy Act* in Alberta;
- collected, used or disclosed solely for personal or domestic (home and family) purposes;
- collected, used or disclosed solely for artistic, literary or journalistic purposes;
- about an individual who has been dead for at least 20 years or contained in a record that came into existence at least 100 years ago; or
- contained in a court file, or in records of a Master, Judge or Justice of a Court of Alberta in compliance with the criteria set by the Act.

**The Act Requires Reasonableness** The Act requires organizations to collect, use and disclose personal information for reasonable purposes only. Moreover, a consent provided by an individual is only valid if the purpose for which the information is collected is reasonable. The test for reasonableness is what a reasonable person would consider appropriate in the circumstances.

**TIP:** It can be difficult for an organization to determine what a “reasonable person would consider appropriate in the circumstances.” What one person considers reasonable may be unreasonable to another. It may be helpful to ask questions, such as:

- Would I want this type of personal information about myself or my family collected, used or disclosed this way? If not, the practice may not be reasonable.
- Have I confirmed that the majority of stakeholders (customers, potential customers) think the

collection, use or disclosure is reasonable in the circumstances? If, for example, the majority of employees did not think a particular use was reasonable, then the organization might want to consider alternatives.

- Would collection, use or disclosure of this type of personal information **benefit**, or be **detrimental** to:
  - the stakeholder (customer, potential customer)?
  - the organization?
  - the general public/society?

If, for example, a disclosure benefits the organization but is detrimental to the stakeholder, it is less likely to be considered reasonable than if it clearly benefits the stakeholder.

Organizations must not mislead individuals about why they are collecting, using, or disclosing personal information. Consent is not valid if it was obtained using false or misleading information, or by using deceptive or misleading practices.

**Example:** An organization operates an Internet website which assists people who are interested in dating. The organization asks individuals for consent to collect their personal information to give to other singles who might be interested in meeting them. The organization says that it will not use the contact information for marketing purposes. Six months later, the organization sells the contact information to another organization to use in marketing romantic products.

### **Understanding Consent Requirements**

Organizations can only collect, use, or disclose personal information as permitted or required by law or with the consent of the individual to whom the personal information relates.

Personal information must be collected directly from the individual, unless the individual consents to collection from other sources.

An organization cannot, as a condition of providing a service, require an individual to consent to the collection, use or disclosure of information beyond what is necessary to provide the service.

Organizations must limit their collection to information that is necessary to provide the service. This is particularly important where the organization wishes to rely upon an “implied” consent through “voluntary” provision of the personal information (see discussion of implied consent below). Implied consent can only apply when the information is collected for obvious purposes.

Consent must be obtained before or at the time of collection, except where the Act provide otherwise. The form of consent must be appropriate to the kind or sensitivity of the information.

Upon giving reasonable notice, and recognizing that there may be consequences, individuals may withdraw or vary their consent at any time.

If organizations want to use personal information that was collected for one purpose for another, secondary purpose, they must obtain consent for the secondary use.

Consent can take different forms including express, implied, or deemed.

**Express  
Consent**

Express consent is the most explicit method of obtaining consent. It may be provided orally or in writing (including electronically), and occurs when an individual specifically agrees to collection, use or disclosure of personal information for specified purposes.

**Example:** While shopping at your favorite drug store, you are asked if you wish to join their loyalty program which provides benefits based on your purchases. You agree and fill out the application form, signing the consent indicating that you agree to the drug store collecting and using your personal information for the purposes identified in the application, and limiting disclosure to related companies identified on the form.

Organizations will most likely comply with the Act's consent requirements if they obtain express, written, consent. However, oral express consent is also valid under the Act.

**Example:** You call for a pizza to be delivered and are asked if the restaurant can collect your telephone number, address and pizza choice to be entered into a database so that the next time you call they can quickly identify you and your preferences. You say "yes."

Oral consent may be appropriate where the consent is easily withdrawn and the implications are minor - for example, where the organization can easily delete information from a database if challenged about whether consent was properly obtained, and if the information has not been disclosed to any other organizations.

**TIP:** If it may be important to have proof of consent, organizations may decide written consent is more appropriate than oral consent. Written consent can be obtained in person, by mail, fax or even e-mail.

When relying on oral consent, organizations should ensure training or other systems are in place so that the request for consent is always given in a consistent manner.

## **Opt-Out Consent**

The Act allows for consent to be either opt-in or opt-out. Opt-in consent is a form of express consent, and occurs when an individual specifically agrees to the collection, use or disclosure.

**Example:** In the previous drug store example, the application form includes an option to receive notices of up-coming sales. Individuals check a box indicating that they wish to receive notices. (**"Opt-In"**)

Opt-out consent occurs when an organization indicates that it will collect, use or disclose information unless the individual indicates otherwise.

**Example:** In the previous drug store example, the application form indicates that the drug store will assume individuals wish to receive promotional

material from related companies unless they check the box which indicates “no” or call a 1-800 phone number to advise that they do not wish to be included. (**“Opt-Out”**)

If relying on opt-out consent, organizations must take into account the sensitivity of the information and the intrusiveness of the use. Where the personal information involved is sensitive (for example, medical or financial information) organizations should obtain **express** consent.

If relying on opt-out consent, organizations must advise the individual of the purposes for which the information is being collected, used and disclosed, and provide the individual with a reasonable opportunity to decline or object.

**Implied Consent** The Act provides for consent to be implied when the purpose for which the personal information will be used is self-evident or obvious, and it is reasonable that an individual would voluntarily provide the information for that purpose

**Example:** You are shopping at the mall and there is a digital camera on display at a store offering film processing. The camera will be awarded to the lucky person whose name is drawn from the entries. You fill out the slip of paper with your name and phone number and drop it in the entry box.

In this example, you have voluntarily provided personal information for the self-evident and reasonable purpose of being contacted if you win.

It would not be reasonable, however, for the organization to use the information for other purposes such as creating a mailing list or being contacted by phone to promote services. These purposes were not stated on the entry slip, and would not be self-evident.

**Information Collected Before January 1,2004** Personal information collected before the Act came into effect on January 1, 2004, is deemed to have been collected with consent, and may be used and disclosed for the purposes for which it was originally collected.

**Example:** An individual provides their name and mailing address to an organization prior to 2004 in order to receive a catalogue; after January 1, 2004, the organization may continue to use the information to send out catalogues. If the organization now wants to use the contact information for a new purpose, however, consent will be required.

If the individual provided personal information in order to receive the catalogue, and has also been receiving marketing material from related companies since that time, the organization should now obtain the individual's consent to disclose the information to the other organizations.

**Consent Must Relate to a Specific Purpose** In order for an individual to consent to a proposed collection, use or disclosure of personal information, the individual must be notified of:

- the purpose(s) for which the organization is collecting, using and disclosing the information, and
- the name of someone who is able to answer on behalf of the organization the individual's questions about the collection.

Notification must occur before or at the time of collection.

**Example:** A professional association includes a statement on its membership application form that states that personal information is collected in order to inform members about activities of the association, communicate with them, mail a newsletter, further the goals of its members, and collect annual fees. The association tells them that it will not disclose personal information to anyone outside the association, except as permitted or required by law. The association further states it will not sell, lease, or barter personal information.

By completing and signing the form, each member consents to the association collecting and using the personal information for the identified purposes.

**TIP:** the association does not need consent to disclose personal information “as permitted or required by law” but, by mentioning this exception in their notification, the association has informed the members of this possibility which may help to reduce concerns.

**TIP:** Organizations need to clearly understand the purposes for which they collect, use or disclose information in order to properly notify the individual when seeking consent. Consent will be valid only if it relates directly to the identified purposes, and is reasonable in the circumstances. If the notification of purpose is too narrow, it may not comply with the requirements of the Act; if it is too broad, it may be either meaningless or deceptive.

Merely notifying individuals that collection is taking place does not meet the requirements for notification under the Act, and therefore cannot be the foundation for a valid consent.

**Example:** A business posts a notice that premises are under video surveillance. While customers and others are aware that collection is taking place, there is no notification of the purpose(s) for collection, use and disclosure, nor is it “self-evident.” Accordingly there is no consent for collection, use or disclosure.

In this situation, the organization may want to state the purposes of collection, use and disclosure in the notice, and provide the name of someone who can be contacted in the event individuals have questions about the surveillance. Even so, the organization must still establish that the surveillance activity is reasonable in the circumstances.

### **Consider the Sensitivity of Information**

The more sensitive personal information is, the greater the organization’s obligation to protect it from misuse. The following are some examples of personal information that may be considered to be sensitive:

- genetic information, drug and alcohol test results and general medical information of all types
- biometric information (fingerprints, retina scans, voice prints)
- sexual orientation
- political or party affiliations
- philosophical beliefs, and religious associations
- unique identifiers, including health card numbers, employee identifications and social insurance numbers
- ethnic, cultural and racial information

The sensitivity of other types of personal information may depend upon factors which are particular to the individual or the context.

**Example:** A subscriber list for a news magazine generally may not be considered sensitive personal information. However, a subscriber list for some special-interest magazines may be considered sensitive as it reveals information about the subscriber. For example, if the magazine was generally subscribed to by wealthy collectors of specialty items, or individuals of a particular religious persuasion.

**Example:** Home addresses are often not recognized as sensitive information, but where the individual is at risk of domestic violence, theft or stalking, the information may be highly sensitive.

Organizations should identify all situations where they are gathering sensitive information to ensure that the appropriate consents have been obtained, and that adequate procedures are in place to prevent misuse.

## **Disclosure**

Many individuals are less concerned about the way an organization will use their personal information, than they are about what information the organization may disclose to another party.

**Example:** An individual consults a debt counseling organization to obtain advice on a financial problem. The individual is comfortable with the counselor knowing details of his situation, but is concerned that

other staff might also read the file. The individual is also concerned that his employer or a creditor might find out that he has financial difficulties.

Organizations should obtain written consent from the individual to disclose information to an outside party, unless the Act provides otherwise. The consent should clearly identify the other parties to which the information is disclosed. While organizations may want to keep the wording as broad as possible so they do not have to ask for consent in future, individuals will be more comfortable with specific wording.

**Collection, Use And Disclosure Without Consent** The Act allows organizations to collect, use and disclose personal information without consent in limited circumstances. These are set out in Sections 14, 17 and 20 of the Act, and include situations where organizations wish to repay or collect on a debt, where collection, use or disclosure is necessary for an investigation, or clearly in the interests of the individual and consent cannot be obtained in a timely way.

**TIP:** Organizations should become familiar with the circumstances under which they may collect, use and disclose personal information without consent. Further discussion and examples of each exception are set out in *The Guide for Businesses and Organizations on the Personal Information Protection Act* which is available through the office or web sites of the Office of the Information and Privacy Commissioner and Access and Privacy Branch, Alberta Government Services.

**Variation or Withdrawal of Consent** An individual may change or withdraw consent with reasonable notice to the organization as long as this does not break a legal duty or promise between the organization and the individual.

**Example:** A customer who has purchased a television and extended warranty from a retail outlet decides that she no longer wishes to receive promotional material for other products. The customer advises the retail outlet that consent for promotional mailings has been withdrawn. The organization must remove her name from the mail-out list within a reasonable time.

**NOTE:** In this example, the customer's consent to use her personal information to honor the extended warranty is still in effect. While the organization must remove her name from the list for promotional mailings, it is reasonable to retain certain information in order to continue to honor the warranty.

If the results of withdrawing or changing the consent are not immediately clear to the individual, the organization must explain them to the individual.

**Notification and Consent Checklist**

Organizations may find it helpful to review the following checklist when establishing consent requirements:

1. Is the information personal information as defined in the Act?
2. If yes, does the Act apply to the personal information?
3. If the personal information is covered by the Act, is consent required for collection, use and disclosure (for example, does the Act allow the organization to collect, use and disclose the information without consent)?
4. If consent is required, what is the appropriate form of consent? (express, implied or opt-out)
5. Where required, has the organization clearly identified the purposes for which it collects, uses, and discloses the information? Are these purposes reasonable?
6. Has the organization developed appropriate procedures to obtain and record consents and to handle withdrawal and variations of consents?
7. Has the organization developed appropriate procedures to authenticate the identity of the individual providing consent?

**Other Resources** For an overview of the Act with examples and tips for incorporating good privacy practices, see *A Guide for Businesses and Organizations on the Personal Information Protection Act*.

*The Personal Information Protection Act, A Summary for Organizations* summarizes the key obligations of organizations.

*Ten Steps to Implement PIPA* is a quick reference for organizations preparing for the Act.

Publications are available at the web site of the Office of the Information and Privacy Commissioner ([www.oipc.ab.ca](http://www.oipc.ab.ca)).

Publications are also available on-line at the Alberta Government Services Information Management, Access and Privacy web site ([www.pipa.gov.ab.ca](http://www.pipa.gov.ab.ca)).

Visit the Queen's Printer web site to view an on-line version of the Act ([www.qp.gov.ab.ca](http://www.qp.gov.ab.ca)).