A Guide for Businesses and Organizations

on the *Personal Information Protection Act*

Produced by Service Alberta and the Office of the Information and Privacy Commissioner

Revised November 2008

Office of the Information and Privacy Commissioner

pipa | Personal Information Protection Act

Alberta

NOTE

This guide was prepared to help organizations implement the *Personal Information Protection Act* which came into effect on January 1, 2004. This guide 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. The guide is not binding on the Office of the Information and Privacy Commissioner of Alberta.

ISBN 0-7785-7480-4

A Guide for Businesses and Organizations

on the *Personal Information Protection Act*

Produced by Service Alberta and the Office of the Information and Privacy Commissioner

Revised November 2008

Office of the Information and Privacy Commissioner

pipa | Personal Information Protection Act

Alberta

Introduction

Welcome to private sector privacy. On January 1, 2004, Canada joined much of the rest of the world in setting standards for the use of personal information by the private sector. The fair information principles involved are universal and pretty straightforward: get consent to collect, use and disclose personal information; don't collect more information than you need to do the job; use it for the purposes for which you collected it; make sure the information is accurate; let people see what information you have on them; keep the information secure and so on. Of course, the devil will be in the details. This guide is meant to deal with the details in a straightforward way.

The *Personal Information Protection Act* requires a lot of "reasonableness." It will take some time, and in certain cases, some trial and error, to get to what is reasonable. The customer might not think the business is being reasonable; the employee might not think the employer is being reasonable (and vice versa). It is important to keep in mind that being reasonable is not a right and wrong, black and white process.

"Reasonableness" results from thinking about the situation, being fair and possibly putting yourself in the other person's shoes. Most times, where there are complaints, the parties will arrive at some agreement on what is reasonable; that is, what reasonable people do. When they cannot, my Office will help.

The advent of this legislation is a good opportunity for organizations to put their "informational houses" in order. Look at the information you collect, why you need it, and what you do with it. Check out those old paper files and databases and those forms you developed years ago. Decide if they are realistic under the Act. In the Information Age, "garbage in" does mean "garbage out"!

Our new legislation is also an opportunity for industry, business, labour and professional organizations to look at industry-wide information practices and develop reasonable standards from which organizations, customers and employees can benefit.

I am particularly pleased that both Alberta and British Columbia have embarked upon almost identical legislative courses and that these courses are intended to be substantially similar to the federal law. This is good for everyone. Hopefully, other provinces will follow suit.

My Office and the Information Management, Access and Privacy Division of Alberta Government Services [renamed Access and Privacy, Service Alberta in 2006] are here to help. We are cooperating on projects such as this guide in unprecedented ways.

Frank Work, Q.C.
Information and Privacy Commissioner of Alberta
February 2004

Contents

Why a guide? **8**

Overview **9**

What does the *Personal Information Protection Act* (PIPA) do? **10**

What organizations and types of information does PIPA regulate? **12**
Organizations under the Act 12
Self-governing professional organizations 12
Non-profit organizations under the Act 13
Information not covered by PIPA 14
How does PIPA affect legal proceedings? 15
Consent is presumed for information collected before January 2004 16
PIPA "trumps" other Acts of Alberta 16
An organization cannot contract out of the PIPA rules 16
Does PIPEDA take priority over PIPA? 17

PIPA guidelines for your organization **18**

1. Be accountable **18**

2. Get consent **20**
Types of consent: express, implied and opt-out 20
Placing reasonable conditions on consent 23
Withdrawing or changing consent 23
Refusing to sell a product or service 23
Getting consent by deception 24

3. Follow the rules for collecting information **25**
Collecting information indirectly 25
Informing the individual why the information is being collected 25
Collecting information from another organization 26
Collecting information without consent 27

4. Follow the rules for using information **29**
Using information without consent 29

5. Follow the rules for disclosing information **31**
Disclosing information without consent 31

6. Follow special rules for employee information **34**

7. Follow special rules for business transactions **36**

8. Follow the rules for giving access to, and correcting, personal information **37**
An individual's general right of access to his or her information 37
Can you charge fees? 38
Who can request personal information? 38
Who is an authorized representative? 39
How do you respond to a request for personal information? 40
Exceptions to giving access 41
Requests for corrections to personal information 43
How to respond to a request for correction 43

9. Follow the rules for accuracy, protection and retention of personal information **44**

How will the Act be enforced? **46**
The Commissioner can investigate complaints and hold inquiries 46
Duty to comply with Commissioner's Orders 47
An organization is protected from liability 47
An employee can blow the whistle on an organization 48
A person can be convicted of an offence under the Act 48
An individual can sue for damages for breach of the Act 49

Definitions of terms used in this guide **50**

Why a guide?

We developed this guide for businesses and other organizations to help you understand the *Personal Information Protection Act* (PIPA or the Act) and the areas of PIPA you are most likely to run across in operating your businesses.

The guide will not answer every question but will cover the major rules in the Act and show how businesses can operate to comply with those rules.

In the guide, we give examples of situations that organizations may face. Some of these examples are based on cases decided by the Information and Privacy Commissioner. Where such examples are used, the citation for the decision is given in brackets. We have boxed the examples to make them easier to find.

The Office of the Information and Privacy Commissioner of Alberta and Access and Privacy, Service Alberta, have published numerous further resources to help organizations and individuals understand their rights and obligations under PIPA. These resources are available on their respective websites: **www.oipc.ab.ca** and **pipa.alberta.ca**.

This guide should not take the place of legal advice. If you are unsure if or how the Act applies, please contact the person in your organization appointed to make sure you follow the Act or a lawyer.

Some words or phrases are in *italics*. They are explained either in the paragraph after they are used or in the Definitions at the end of the guide. It is important to pay attention to the definitions in the Act when you are trying to decide if or how the Act applies.

Contact information for this guide:

Access and Privacy
Service Alberta
3rd Floor, 10155 – 102 Street
Edmonton, Alberta T5J 4L4
Phone: 780-644-PIPA (7472)
Toll free dial 310-0000 first
E-mail: **pspinfo@gov.ab.ca**
Website: **pipa.alberta.ca**

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

Overview

Surveys conducted by the Office of the Information and Privacy Commissioner show that Albertans place a high value on their privacy. Good privacy practices give businesses a competitive edge. So it makes good business sense for organizations to do what is needed to protect privacy.

The *Personal Information Protection Act* (PIPA) came into effect on January 1, 2004. PIPA aims to protect the personal information of an organization's customers and its employees. The Act's rules balance:

- an individual's right to have his or her personal information protected, and
- the organization's need to collect, use and disclose personal information for purposes that are reasonable.

PIPA also gives individuals the right to ask an organization to see the personal information it has about them, to find out how it is being used and disclosed, and to ask for corrections if they believe a mistake has been made.

In many areas of the Act, PIPA uses a test of what is ***reasonable***. This means what a reasonable person would think is appropriate in the situation.

PIPA applies to organizations, such as incorporated or unincorporated businesses, trade unions, partnerships, and individuals running their own businesses, and to persons acting for them, such as agents or contractors. There are special sections of the Act dealing with *non-profit organizations* and *professional regulatory organizations*. The Act does not apply to public bodies under the *Freedom of Information and Protection of Privacy Act* (FOIP Act), such as government departments, universities, public school boards, hospitals and municipalities. Nor does it apply to personal information used for personal, family or home purposes. Exclusions from the Act are discussed later in the guide.

Organizations have to take care of personal information that is **in their *custody* or under their *control***. This includes information in the organization's offices, in its files or laptops when staff travel or in the hands of contractors or data processors, for example. Organizations have to follow the rules in the Act about consent and about collecting, using and disclosing personal information. The Act is written with collection, use and disclosure of personal information addressed in separate sections. However, many of the rules about collection are the same as the rules dealing with use and disclosure.

What does the *Personal Information Protection Act* do?

PIPA is an act about privacy in the private sector. It helps protect the personal information of the public (your customers) and your employees. It creates common-sense rules about collecting, using and disclosing (showing, telling or giving some other organization) personal information. The Act balances:

- an individual's right to have his or her personal information protected, and
- an organization's need to collect, use or disclose personal information for purposes that are reasonable, that is, for legitimate business purposes (section 3).

The Act also gives individuals the right to ask an organization to show them the personal information it has about them and to ask for the information to be corrected if they think the information is incomplete or inaccurate.

Personal information means information that can identify an individual (for example, name, home address, home phone number, e-mail address, ID numbers), and information about an individual (for example, physical description, educational qualifications, blood type). For PIPA to apply, the personal information in question must be about an individual, identify an individual, or be able to identify an individual.

Business contact information is a sub-set of personal information. It includes an individual's name and position or title, business telephone number, business address, business e-mail, business fax number and other business contact information. This information can be disclosed without consent to allow an individual to be contacted as a representative of their organization. For example, a Chamber of Commerce can list its board members on its website and a company can list its sales representatives in a marketing brochure.

To understand what purposes are reasonable, consider the reasonable person test in the context of the following examples:

EXAMPLE

A customer returns an item to a store without a receipt. It is reasonable for the store clerk to request the customer's driver's licence to verify her identity. It would not be reasonable for the store clerk to record the driver's licence number and put it on file to be retained indefinitely (*Investigation Report P2005-IR-007*).

EXAMPLE

Mark has a credit card with an Alberta retailer and also has bought furniture from the retailer on a "do not pay for 12 months" arrangement. Mark has worked for the store for two summers while attending school. It is reasonable for Mark to request a copy of all his personal information held by the retailer.

The retailer must search for the credit and employment information, both paper and electronic files, wherever it is likely to be in the organization, and make a copy of it for Mark within 45 days.

EXAMPLE

An individual is asked to fill out a tenant application form. On the form, the landlord asks for the applicant's Social Insurance Number and bank account number, so the landlord can "cross-check" information on the applicant's credit report. The landlord needs to screen prospective tenants, but requiring this type of personal information is not reasonable for this purpose. Obtaining references from former landlords would be a less privacy-invasive way of determining an applicant's reliability (*PIPA Case Summary P2006-CS-013*).

EXAMPLE

Susan is buying a new truck and applies to the dealer for financing. The dealer can ask Susan to provide personal information to process the loan, and can use and disclose the information as required to process the loan application. However, it would be unreasonable for the dealer to ask for personal information that is either irrelevant to the purchase or for processing the loan application, or to use or disclose the personal information for some other purpose.

The Act applies to personal information whether the information is recorded or not. For example, the Act applies when an employee discloses personal information of a customer over the phone. However, the right of access and correction only applies to personal information that has been recorded.

The Act does not apply to general information used to operate the business of the organization, or to the use of non-identifiable or **aggregate information** such as statistical information about groups of individuals.

For more information, see **Information Sheet 3: Personal Information**, available at **pipa.alberta.ca**.

What organizations and types of information does PIPA regulate?

Organizations under the Act

PIPA applies to all *organizations* and to all personal information held by organizations unless the Act says that it does not apply (section 4(1)).

An ***organization*** includes:

- a corporation,
- an association that is not incorporated,
- a trade union,
- a partnership, and
- an individual acting in a commercial capacity (for example, an individual running a small renovation business that is not incorporated).

When Organization A hires Organization B under a contract, Organization A is responsible for the personal information related to the contract. Organization B is also responsible for making sure they operate in accordance with the Act.

An *organization* does not include a person who is acting in a personal or domestic way, related solely to family or home activities.

Self-governing professional organizations

PIPA allows a professional regulatory organization to develop a personal information code that provides the same level of privacy protection as the Act while allowing some latitude in format and wording. The code must be consistent with the rights and obligations set out in PIPA, and the Commissioner can still investigate or review the decisions or actions of a professional regulatory organization with a personal information code.

For guidelines on developing a personal information code, see **Guidelines for Developing a Personal Information Code for Professional Regulatory Organizations**, available at **pipa.alberta.ca.**

Non-profit organizations under the Act

The Act defines what is a ***non-profit organization*** for the purpose of applying the Act. A non-profit organization is defined as an organization incorporated under the *Societies Act* or the *Agricultural Societies Act,* or registered under Part 9 of the *Companies Act*. For these organizations, the Act applies only when they collect, use or disclose personal information in connection with a commercial activity (section 56).

PIPA applies to other organizations that are not incorporated as described above, whether they are not-for-profit or for-profit organizations.

A ***commercial activity*** means a transaction, act or conduct that has a commercial character to it, such as selling, bartering or leasing donor, membership or other fund-raising lists. It also includes operating a private school or college or an early childhood services program.

The Act does not apply to the personal information of employees or volunteers of a non-profit organization. Nor does it apply to personal information collected during a transaction that is not a commercial activity.

EXAMPLE

A community hockey team incorporated under the *Societies Act* runs a raffle to buy equipment for the club. Ticket buyers provide their name, address and phone number on the ticket stub. The team later compiles a list of ticket purchasers and sells it to the local sports equipment store. This sale of personal information is a commercial activity. The rules for collecting, using and disclosing personal information apply here. The team needs each ticket buyer's consent to sell the contact information to the sports equipment store.

EXAMPLE

A society runs a fitness facility; patrons can use the facility only after paying a daily, monthly or annual fee. The Act applies to collecting the personal information of registrants. The society must obtain consent when individuals register for fitness classes (see *IPC Order P2006-008*).

For more information, see **Information Sheet 1: Non-Profit Organizations**, available at **pipa.alberta.ca**.

Information not covered by PIPA

Section 4 of the Act lists certain purposes, organizations or types of records containing personal information where the Act does not apply. The more common exclusions are described below.

PIPA does not apply if you collect, use or disclose personal information for certain purposes. These include:

- for home or family purposes (for example, for Christmas card mailing lists),
- for artistic or literary purposes, or
- for journalistic purposes (this protects freedom of expression for newspapers, but PIPA does apply to purposes such as the marketing of a newspaper).

PIPA also does not apply to personal information that is collected, used or disclosed:

- by a registered constituency association or a registered political party,
- by an individual running for public office, for campaigning purposes, or
- that is business contact information collected, used or disclosed for the purpose of contacting an individual as a representative of an organization.

Below are examples of personal information to which the Act does not apply.

EXAMPLE

Guy is writing a historical article that will be published in a trade journal. He can collect, use and disclose personal information without following the rules set out in the Act. The Act does not apply to journalistic activities. Organizations providing information to Guy for his research can release personal information about individuals who died 20 years ago or more, as PIPA also excludes such information.

Public bodies subject to the *Freedom of Information and Protection of Privacy Act* (FOIP Act) are not organizations regulated by the Act. These public bodies include government departments, municipalities, universities, public colleges, and public school boards. PIPA does not apply to personal information held by a public body.

Certain kinds of personal information are also excluded from PIPA. Some of the most common examples of personal information to which PIPA does not apply are:

- if the FOIP Act applies to the information (for example, when a government department discloses personal information to a contractor carrying out work for that department, the FOIP Act applies to the information)
- if the information is health information and the *Health Information Act* applies to that information
- if the information is about an individual who has been dead for 20 years or more or in a record that is 100 years old or older
- if the information is personal information in court files

EXAMPLE

An accounting firm handles payroll information for a municipality. It receives the names of employees, their Social Insurance Numbers, hours of work and rates of pay from the municipality. The municipality is under Alberta's *Freedom of Information and Protection of Privacy Act* (FOIP Act). The payroll information stays under the control of the municipality and the FOIP Act. However, PIPA applies to information the accounting firm receives from private-sector clients, as well as the firm's own administrative records (for example, information about its employees).

TIP

When working under contract for a *public body,* organizations should be clear whether the public body or the organization has control of personal information generated under the contract. This should be specified in the contract.

How does PIPA affect legal proceedings?

Lawyers must follow rules and laws about how certain information is handled. PIPA does not affect those rules or laws. Also, parties to ***legal proceedings*** have a right to get certain information by law, for example, through examinations for discovery. PIPA does not change that right (section 4(5)). Information created by judges and the courts is not covered by PIPA.

Consent is presumed for information collected before January 2004

The Act considers personal information collected by an organization before January 1, 2004 to have been collected with consent. The organization may continue to use and disclose the information for the original purpose for which it was collected. For example, if a customer's name and contact information was collected to offer a warranty on a product, the information can continue to be used and disclosed to administer the warranty.

If an organization wants to use the information for a purpose unrelated to the original collection, the organization will need to obtain a new consent. For example, if the organization provides customer information to a charitable organization it supports, it may not be reasonable to consider this disclosure to be part of the original purpose for collecting the information. New consent would be required to disclose the customer information to the charitable organization.

In deciding when to rely on this provision, and when to obtain a new consent, consider also whether the information collected before January 2004 could now be collected in accordance with the Act. For instance, if it would be unreasonable to collect an individual's Social Insurance Number for a certain purpose now that the Act is in effect, it would not be advisable to continue to use the number for that purpose.

The general rules in the Act about protecting personal information, giving an individual access to his or her information, as well as limiting use and disclosure, apply regardless of when the information was collected (section 4(4)).

For more information, see **Information Sheet 4: Personal Information Collected Before 2004**, available at **pipa.alberta.ca**.

PIPA "trumps" other Acts of Alberta

If a section in PIPA conflicts with another act or regulation, the section in PIPA must be followed unless the other act is the FOIP Act (section 4(6)), or unless the Act or the PIPA Regulation states that PIPA does not apply. Currently there are no such provisions in other Alberta acts or the PIPA Regulation.

An organization cannot contract out of the PIPA rules

An agreement, contract or release that says an organization does not have to follow PIPA has no legal effect (section 4(7)).

Does PIPEDA take priority over PIPA?

Both the federal Act, the *Personal Information Protection and Electronic Documents Act* (PIPEDA), and Alberta's *Personal Information Protection Act* (PIPA) focus on protecting personal information in the private sector.

PIPEDA applies to every organization across Canada when collecting, using or disclosing personal information while carrying out a commercial activity within a province, unless a province passes legislation that is substantially similar to PIPEDA (based on the same purposes and rules).

PIPA is Alberta's own private-sector privacy Act, and has been designated substantially similar to PIPEDA. It applies to provincially-regulated private businesses, *non-profit organizations*, trade unions and self-governing professions doing business inside Alberta. PIPEDA also applies to these organizations when carrying out commercial activities involving personal information that crosses Alberta's borders. PIPEDA continues to apply to federally-regulated industries located in Alberta, such as banks, telephone companies, and interprovincial trucking companies.

EXAMPLE

An individual applies for credit when buying a new computer. The individual agrees that the store can conduct a credit check. The store discloses the individual's personal information to the credit reporting agency in Ontario. The disclosure of the personal information to the Ontario organization makes the transaction subject to PIPEDA.

EXAMPLE

An Alberta company, AB&C Counselling, provides counselling services to employees of an airline under an employee assistance program. AB&C is obliged by law to follow PIPEDA rules regarding the personal information of the airline's employees because the airline is a federally-regulated undertaking. However, as an Alberta-based company, AB&C will follow PIPA for the rest of its operations (for example, payroll processes, services provided to individuals or organizations in Alberta).

For more information on the application of PIPEDA and PIPA, see **Questions and Answers regarding the application of PIPEDA, Alberta and British Columbia's *Personal Information Protection Acts* (PIPAs)**, available at **www.oipc.ab.ca**.

PIPA guidelines for your organization

1 Be accountable

Bottom line: Your organization is responsible for all the personal information that is either in your *custody* or under your *control* (section 5). Organizations have ***custody*** of personal information when it is in their offices, facilities, file cabinets, computers, portable electronic storage devices, and so on.

Personal information is under the ***control*** of an organization when the organization can decide how to use, disclose, and store it, and how long to keep it. For example, if your organization sends electronic information (data) to another business to process or store it, the information is still under your control. You are obliged under PIPA to make sure that the other business protects it the same way as you do. The other business will still be responsible for ensuring its own compliance with the Act.

EXAMPLE

An event planner contracted with a ticket agency to sell tickets to patrons. Both organizations are responsible for ensuring that personal information collected, used and disclosed during the sale of event tickets followed the rules under PIPA (see *IPC Investigation Report P2007-IR-007*).

Your organization must designate one or more individuals to make sure that the organization follows the rules in PIPA. The(se) individual(s) may also be the contact person(s) for answering questions about the Act and for taking access requests and complaints under the Act. Other individuals in your organization may be delegated to act in the place of the appointed individual(s).

You need to develop, and put into practice, policies and procedures to protect personal information. The policies and procedures should cover:

- what personal information you collect
- how you obtain consent for collecting, using and disclosing personal information
- how you use and disclose personal information
- how you ensure that adequate security measures are in place
- how you process access requests
- how you respond to enquiries and complaints

To be accountable, your organization must do what a reasonable person would do in the situation. That means reviewing your personal information handling practices for both ongoing and new activities.

Use the following questions to understand your personal information handling practices:

1. What personal information do we collect?
2. Why do we collect it?
3. How do we collect it?
4. What do we use it for?
5. Where do we keep it?
6. How is it secured?
7. Who has access to or uses it?
8. To whom is it disclosed?
9. When is it disposed of?
10. In light of PIPA, should we change any of these practices?

TIPS

- **Support the privacy officer**
  Have senior management support the designated privacy officer and give him or her the authority to deal with privacy issues related to your operations.
- **Advertise the identity of the privacy officer**
  Make sure that all staff know who the designated privacy officer is and include his or her contact information on your website.
- **Analyze your own practices**
  Analyze your business's personal information handling practices. Make sure they meet fair information principles (see sections on collection, use, disclosure, protection).
- **Develop and implement privacy policies**
  Implement policies and procedures to protect personal information.
- **Insert privacy clauses in agreements**
  Include a privacy protection clause in contracts to make sure that the contractor protects personal information the way your organization does.
- **Inform staff**
  Inform and train staff on privacy policies and procedures.
- **Communicate your privacy policies**
  Make information available explaining your policies and procedures (for example, in brochures and on websites).

For more information, see **Personal Information Protection Policy for Small and Medium Size Businesses**, available at **pipa.alberta.ca**.

2 Get consent

Bottom line: Unless the Act says that you don't need consent, you **must** get consent to:

- collect personal information,
- collect personal information from someone other than the individual the information is about,
- use personal information, or
- disclose personal information (section 7).

Usually consent is obtained at the time the personal information is collected.

Keep in mind that consent from an individual will not authorize the collection of personal information if the collection is not reasonable (see *IPC Order P2006-011*).

Types of consent

The three types of consent are:

a. express consent,
b. implied consent, and
c. consent by not opting out (section 8).

Your organization should choose the form of consent that is appropriate for the transaction or activity. Consider what an individual would reasonably expect, the circumstances, and the sensitivity of the information.

When relying on either express consent or opt-out consent, your organization must give the individual enough information about the collection of his or her personal information, so the individual can make an informed decision whether to give consent. This notification requirement is discussed further under Guideline 3.

a. Express consent

Giving consent in writing or verbally is express consent. Written consent may be given electronically (by fax or e-mail) as long as the organization receiving the consent is able to make a copy of the consent on paper.

EXAMPLE

A customer signs up for a loyalty card at a grocery store to obtain lower prices and special offers. The consent form explains all the uses and disclosures of her personal information, and the customer signs the form giving her consent.

EXAMPLE

An organization provides family counselling for couples considering divorce. Hank and Celeste sign consent forms outlining how the organization will collect, use and disclose this sensitive personal information.

EXAMPLE

A company calls a customer to offer an extended warranty on a product the customer purchased. The customer decides to purchase the warranty. The operator asks whether the company can tape the call to verify the transaction. The customer provides consent orally.

b. Implied consent

Implied consent happens when an individual doesn't actually give consent but volunteers the information for an obvious purpose, and a reasonable person would think that it was appropriate in the situation to volunteer that information.

The Act does not require an organization to provide notice when collecting personal information relying on implied consent (section 13(4)). This is because an organization may rely on implied consent only where it is obvious how the information will be used or disclosed by the organization. Any further use or disclosure of the information that is **not** obvious would require either express or opt-out consent.

If an individual volunteers more personal information than is needed for the purpose(s), the organization cannot collect, use or disclose that extra information. Below are examples of when implied consent can and cannot be used.

EXAMPLE

An individual takes his suit to the dry cleaner. The dry cleaner asks for his name and a phone number. The individual provides these voluntarily. Consent is implied that the cleaner can use the name and phone number to identify the individual when he returns to collect his suit, or to contact him if he forgets to pick it up.

EXAMPLE

If the dry cleaner wanted to use the individual's phone number for marketing purposes at a later time, the dry cleaner would have to inform the individual of this purpose and obtain his consent for that purpose.

c. Opt-out consent

In some situations, an individual can be given the choice to opt out of the collection, use or disclosure of his or her personal information. By not opting out, he or she has provided consent for the organization to collect, use or disclose personal information for the specified purpose.

For example, individuals can ask the organization not to use their names and addresses to send them information about other products by using a check-off box. If an individual does not check off the box, the organization takes this to mean that he or she consents to the organization sending them information about other products.

You can only use opt-out consent by meeting the conditions below:

- your organization must let the individual know why it is going to collect, use or disclose the information
- your organization must give an easy-to-understand notice before, or at the time, it collects, uses or discloses the information
- the individual must have a reasonable chance to say no to the collection, use or disclosure (in terms of format, procedure and time)
- the personal information must not be so sensitive that it would be unreasonable for the organization to use an opt-out form of consent to collect, use or disclose the information

EXAMPLE

Aaron enters a draw to win a computer. He provides his name and home e-mail address. The draw form clearly provides a space to check off if he does not want to receive more information about similar products from the company.

EXAMPLE

Paulette signs up to take a Spanish course at a language academy. The registration form indicates her name and address will be added to the academy's mailing list for future course calendars. She is given the option to check off a box to indicate that she does not want to receive future calendars.

Placing reasonable conditions on consent

An individual can put reasonable terms and conditions on his or her consent. For example, the individual may say that the organization can use the personal information to supply one specific product to the individual but not use it in the future to market new related products (section 7(3)).

Withdrawing or changing consent

An individual may change or withdraw his or her consent by giving the organization reasonable notice of this, as long as this does not interfere with a legal duty or obligation between any two parties (section 9).

If the results of changing or withdrawing the consent are not clear, the organization must let the individual know what the consequences will be. For example, if withdrawing consent means the organization will no longer honour an extended warranty, they should inform the customer of this consequence.

Refusing to sell a product or service

An organization cannot make an individual's consent to collect, use or disclose personal information a condition of supplying him or her with a product or service, if the organization is asking the individual to consent to something that is beyond what is needed to supply that product or service (section 7(2)).

EXAMPLE

A customer was purchasing a product online. Before the online store would process the transaction, the retailer required the customer to consent to the use and disclosure of his personal information for marketing purposes. This is not a reasonable practice under PIPA (see *IPC Investigation Report P2007-IR-007*).

EXAMPLE

A telephone company refused to provide cell phone service to a customer because the customer would not provide his Social Insurance Number for a credit check. The federal Privacy Commissioner found that this was unreasonable (see *PIPEDA Case Summary #151*).

Getting consent by deception

An organization cannot get consent by a false or misleading means or by misleading the individual about why it is collecting, using or disclosing the information. If this happens, the consent is **not legal** (section 10). An example of an organization gaining illegal consent follows:

EXAMPLE

An individual receives a survey in the mail asking for his opinions on current events. It includes an optional section for the individual's name and address, and a series of questions about household purchases over the last three months. The survey form indicates that the organization will send discount coupons tailored to each survey respondent as a thank-you for completing the survey. The company then sells the information to marketers. The company did not have consent to sell the individual's name and address for marketing purposes.

TIPS

- **Obtain consent in writing or orally, in person, by phone, by mail, through a website, etc.**
- **Make consent clauses easy to find, easy to understand, and as specific as possible about uses and disclosures.**
- **Choose the type of consent used by considering the reasonable expectations of the individual, the circumstances surrounding the collection, and the sensitivity of the information.**
- **Use express consent whenever possible and in all cases when the personal information is sensitive.**
- **For an individual who is a minor, seriously ill, or mentally incapacitated, obtain consent from a legal guardian or person having a power of attorney or trusteeship order.**

For further information, see **PIPA Advisory 1 - Consent**, available at **www.oipc.ab.ca**.

Follow the rules for collecting information 3

Bottom line: An organization may collect personal information only for purposes that are reasonable and may only collect information that is reasonable for carrying out those purposes (section 11).

Limit the information you collect to what is necessary for carrying out your organization's obligations. Limit both the amount and type of information collected. Doing so benefits an organization because it lessens:

- the risk of not properly using or disclosing personal information, and
- the cost of collecting, storing and retaining unnecessary information.

Ideally, organizations should collect personal information directly from the individual the information is about.

Collecting information indirectly

If the Act allows personal information to be collected without consent, the collection can be from someone other than the individual (section 12).

Informing the individual why information is being collected

Before or at the time of collecting personal information from an individual, you must let the individual know the purposes of the information collection and provide contact information for a person who can answer questions about the collection (section 13(1)). You should define your purposes for collecting personal information as clearly and narrowly as possible so the individual can understand how the organization will use or disclose the information. Avoid overly broad statements.

Examples of specific purposes include opening an account, verifying creditworthiness, providing benefits to employees, processing a magazine subscription, sending out association membership information, guaranteeing a travel reservation, identifying customer preferences or establishing customer eligibility for special offers or discounts.

You may put the notice in writing (for example, on a form or in a related section of a website) or give it verbally (for example, in person or during a phone call). A sample notice is provided on the next page.

SAMPLE OF AN INFORMATION COLLECTION NOTICE

Use the following sample wording, if applicable:

When you first become a customer of XYZ Company, or when you apply for more products and services from us, we will collect your name, address and telephone number (or other necessary personal information) and use it to:

- confirm your identity and credit history;
- open an account with us;
- establish your eligibility for special offers or discounts; and
- provide ongoing service.

We may disclose your personal information:

- to a person who we are satisfied is requesting the information on your behalf;
- to other business units of XYZ Company to help serve you better;
- to a credit reporting agency;
- when permitted or required by law; or
- to a public authority if, in our reasonable judgment, there appears to be an imminent danger which could be avoided by disclosing the information.

If you have any questions about the collection of your personal information, call _____ (give name) at _____ (give phone number) from _____ (give business hours).

Collecting information from another organization

An individual can consent to your organization collecting his or her personal information from another organization. You must be able to show that you received consent. You must satisfy the disclosing organization that the consent follows the rules in the Act, as in the following example.

EXAMPLE

Jim wants to move to a new apartment. He can give the prospective landlord permission to contact his current landlord to obtain a reference. The current landlord needs to know that Jim consented to the reference before disclosing the information.

Collecting information without consent

The Act allows you to collect personal information without consent in certain situations listed in section 14:

a. If a reasonable person would consider that it is clearly in the interest of the individual and consent cannot be obtained in a timely way or the individual would not reasonably be expected to refuse consent
EXAMPLE: A skydiving company can collect the name and phone number for an emergency contact person from its clients.

b. If another Act or regulation requires or allows for collecting information without consent
EXAMPLE: An Alberta credit union can collect an individual's Social Insurance Number as required by the *Income Tax Act* to issue a T-slip.
EXAMPLE: A professional association is permitted under its governing legislation to collect personal information about members when dealing with a complaint from the public.

c. If the information is provided by a *public body* under an enactment of Alberta or Canada
EXAMPLE: An organization provides services to a client of a government social service program and is paid directly by the government department under the *Income and Employment Supports Act*. The government department can disclose information about the client that is necessary to pay for the service, and the organization can collect that information without the consent of the client.

d. If the collection is reasonable for the purposes of an *investigation* or *legal proceeding*
EXAMPLE: An insurer was permitted to collect an insurance claimant's financial history when it had reasonable grounds to suspect fraudulent activity. However, other personal information collected as part of the normal claims procedure required consent, since a standard insurance claim is **not** an investigation under PIPA (see *IPC Investigation Report P2008-IR-001*).

e. If the personal information is *publicly available* as defined in the PIPA Regulation
EXAMPLE: A company may obtain a land title search for a property it is considering purchasing.

f. If the information is necessary to decide whether an individual is suitable for an honour, award or other similar benefit, including an honorary degree, scholarship or bursary (but not for a job or a promotion)
EXAMPLE: A Chamber of Commerce can gather biographical information to provide an achievement award to a member.

g. If a credit reporting agency collects personal information to create a credit report, and the individual has told the organization that originally collected the information that the organization may disclose that information to the credit reporting agency
EXAMPLE: A credit reporting agency can collect a customer's personal information from a department store when the customer applies for the department store credit card and tells the store that it may give his information to the credit reporting agency.

h. If, under the disclosure section of PIPA (section 20), an organization can disclose the information to your organization without consent
EXAMPLE: An organization can collect information about a candidate for a Chamber of Commerce award so the organization can provide a relevant testimonial about the member's accomplishments.

i. If your organization needs the information to collect a debt owing to your organization or to repay the individual money you owe
EXAMPLE: A company can collect an individual's new address from Canada Post to collect a debt.

j. If the organization collecting the information is an *archival institution* and the collection is reasonable for *archival purposes* or research
EXAMPLE: An archive can accept documents containing personal information to preserve them for posterity.

k. If the collection meets the requirements for *archival purposes* set out in the PIPA Regulation and it is not reasonable to obtain the individual's consent. *Archival purposes* is defined in the PIPA Regulation
EXAMPLE: An organization can purchase a historical document concerning the history of the organization at auction to transfer to an archival institution.

Follow the rules for using information 4

Bottom line: An organization may only use personal information for purposes that are reasonable and may only use information that is reasonable to carry out those purposes (section 16).

An organization may only use personal information for the purposes identified in the notice provided to the individual, unless the Act permits otherwise. An organization that collected a customer's address for invoice and delivery purposes cannot use the address to send marketing material without consent for that purpose.

Sometimes it is hard to decide what is a "use" and what is a "disclosure" of personal information. The following explanations may help.

Using personal information usually means using it internally to carry out the organization's purposes. These include providing a product or service or evaluating whether an individual is eligible for a discount. Normally, an organization or its contractors use information within the organization. It would be valid for a shipping department to use customer information that was collected by the billing department.

Disclosing personal information means showing, sending, telling or giving some other organization or individual the personal information in question. Information is disclosed externally when provided outside the organization. To continue the example above, providing the customer's name and address when requested by Canada Revenue Agency would be a valid disclosure of personal information.

Using information without consent

The Act allows you to use personal information without consent in certain situations listed in section 17.

a. When a reasonable person would consider that it is clearly in the interests of the individual and the organization cannot obtain consent in a timely way or the individual would not reasonably be expected to refuse consent
EXAMPLE: A skydiving company can use the emergency contact information given by a client to notify a family member of an emergency situation.

b. When another Act or regulation requires or allows the use without consent
EXAMPLE: An Alberta credit union can use an individual's Social Insurance Number as required by the *Income Tax Act* to print a T-slip.
EXAMPLE: A professional association is permitted under its governing legislation to use information from a complainant to make a decision about a regulated member.

c. When the information was collected from a *public body* that disclosed it under an enactment of Alberta and Canada
EXAMPLE: An organization providing services to a client of a government social service program can use information provided by the government department under the *Income and Employment Supports Act* to process payment for the service.

d. If the use is reasonable for the purposes of an *investigation* or *legal proceeding*
EXAMPLE: An insurer can use information about an insurance claimant's financial history to investigate suspected fraudulent activity.

e. If the personal information is *publicly available* as defined in the PIPA Regulation
EXAMPLE: A company can use information obtained from a land title search when determining whether to purchase property.

f. If the information is necessary to decide whether an individual is suitable for an honour, award or other similar benefit, including an honorary degree, scholarship or bursary (but not for a job or a promotion)
EXAMPLE: A Chamber of Commerce may use biographical information in its files to provide an achievement award to a member.

g. If a credit reporting agency uses personal information to create a credit report, and the individual has told the organization that originally collected the information that the organization may disclose that information to the credit reporting agency
EXAMPLE: A credit reporting agency can create a credit report for a department store, at the request of a customer who is applying for a store credit card.

h. If, under the disclosure section of PIPA (section 20), an organization can disclose the information to your organization without consent
EXAMPLE: The owner of a campground can use the name of an injured hiker disclosed by an Adventure Hiking tour guide to locate the hiker's family members also camping on the grounds, and inform them of the incident (disclosure under section 20(h)).

i. If your organization uses the information to respond to an emergency that threatens the life, health or security of an individual or the public
EXAMPLE: A patron of a recreational facility makes a threat against a facility employee on a customer satisfaction form. The facility can use the patron's information to prevent the employee from being injured.

j. If your organization needs the information to collect a debt or to repay the individual money
EXAMPLE: A company can use an individual's address to collect a debt.

k. If the organization using the information is an *archival institution* and the use is reasonable for *archival purposes* or research
EXAMPLE: An archive may use the personal information in documents to decide how to organize them.

l. If the use meets the requirements for *archival purposes* set out in the PIPA Regulation and it is not reasonable to obtain the individual's consent. *Archival purposes* is defined in the PIPA Regulation
EXAMPLE: An organization can prepare records containing personal information for an appraisal to decide whether the records should be permanently preserved.

Follow the rules for disclosing information 5

Bottom line: An organization may only disclose personal information for purposes that are reasonable and may only disclose information that is reasonable to carry out those purposes (section 19). An organization may only disclose personal information for the purposes identified in the notice provided to the individual, unless disclosure is otherwise authorized under the Act.

Disclosing information without consent

The Act allows you to disclose personal information without consent in certain situations in section 20:

a. **If a reasonable person would consider that it is clearly in the interests of the individual and consent cannot be obtained in a timely way or the individual would not reasonably be expected to refuse consent**
EXAMPLE: An employee of an apartment building was authorized to disclose medical information about a tenant to 911 dispatch and ambulance attendants when the employee heard the tenant's home alarm and became concerned for the tenant's well-being (see *IPC Order P2005-003*).

b. **If another Act or regulation requires or allows the disclosure without consent**
EXAMPLE: An Alberta credit union may disclose an individual's Social Insurance Number as required by the *Income Tax Act* to prepare a T-slip.

c. **If disclosed to a *public body* that is authorized to collect the information under an enactment of Alberta or Canada**
EXAMPLE: A professional health association can give personal information about its regulated members to the Minister of Health and Wellness, since the Minister is authorized by regulation to collect the information.

d. **If a treaty requires or allows for disclosure without consent and the treaty is made under an Act or regulation of Alberta or Canada**

e. **If the disclosure is necessary to comply with a subpoena, warrant or court order that requires information to be produced or with a rule of court relating to the production of information**
EXAMPLE: An organization can disclose personal information when a court order is served on the organization.

f. If a public body or police service needs help in an investigation leading to a law enforcement proceeding or from which a law enforcement proceeding is likely
EXAMPLE: A construction company may provide information to Workplace Health and Safety staff who are investigating a workplace accident.
EXAMPLE: A car dealership can give the tapes from its parking lot security cameras to police investigating a robbery.

g. If the information is disclosed to respond to an emergency that threatens the life, health or security of an individual or the public
EXAMPLE: If a patron of a recreational facility makes a serious threat against a facility employee, the facility manager may disclose the patron's personal information to the appropriate agency to prevent the employee from being injured.

h. If disclosure is needed to contact next of kin or a friend of an injured, ill or deceased individual
EXAMPLE: A mountain climbing tour company can disclose a client's personal information so that a family member may be informed about a client's injury.

i. If the information is needed to collect a debt owing to your organization or for the organization to repay an individual money owed by the organization
EXAMPLE: A company can disclose an individual's former address in order to obtain a forwarding address, so that it can repay a debt to the individual.
EXAMPLE: A retail store cannot post pictures of customers with overdue accounts in order to collect a debt (see *IPC Case Summary P2005-CS-001*).

j. If the information is *publicly available* information as defined in the PIPA Regulation
EXAMPLE: A private college may give a new student the names of health providers in the community, obtained from a professional registry.

k. If the disclosure is to the surviving spouse or adult partner or to a relative of an individual who has died, and if the disclosure is reasonable
EXAMPLE: An organization may disclose information surrounding the circumstances of an individual's death on the organization's premises to close family members.

l. If the disclosure is necessary to decide whether an individual is suitable for an honour, award or other similar benefit, including an honorary degree, scholarship or bursary (but not for a job or a promotion)
EXAMPLE: A Chamber of Commerce can disclose biographical information in its files to another organization to enable that organization to comment on a proposal to give an achievement award to a member of the Chamber of Commerce.

m. If the disclosure is reasonable for the purposes of an *investigation* or *legal proceeding*
EXAMPLE: An insurer can disclose a client's claims history in the process of investigating suspected fraudulent activity.

n. If the disclosure protects against, prevents, suppresses or detects fraud, and the organization disclosing the information is allowed or has been given the power to carry out this purpose under an Act or regulation of Alberta or Canada
EXAMPLE: An organization can disclose personal information requested by the Bank Crime Prevention and Investigation Office of the Canadian Bankers Association for the purpose of a fraud investigation.

o. If a credit reporting agency discloses personal information to create a credit report as permitted by the *Fair Trading Act*
EXAMPLE: A credit reporting agency may disclose a customer's personal information to a department store that is considering the customer's application for the store credit card.

p. If the organization disclosing the information is an *archival institution* and the disclosure is reasonable for *archival purposes* or research
EXAMPLE: An archive can disclose the personal information in documents for research purposes.

q. If the disclosure meets the requirements for *archival purposes* or research set out in the PIPA Regulation and it is not reasonable to obtain the individual's consent
EXAMPLE: An organization may disclose personal information to an *archival institution* for permanent preservation.

6 Follow special rules for employee information

Bottom line: An organization may collect, use and disclose employee information without consent for reasonable purposes related to recruiting, managing or terminating personnel.

An ***employee*** is someone employed by the organization or someone who performs a service for the organization and includes:

- an apprentice
- a volunteer
- a participant
- a work experience or co-op student
- an individual (not a company) acting as a contractor to perform a service for an organization or an individual (not a company) acting as an agent for an organization

Personal employee information means personal information that is reasonably needed to establish, manage or end a work or volunteer work relationship. It does not include personal information that is not related to the relationship.

Managing personnel means the carrying out of that part of human resource management relating to the duties and responsibilities of employees. It can also refer to administering personnel, and includes activities such as payroll and succession planning.

An organization may collect (section 15) or use (section 18) personal employee information without consent when:

- the individual is an *employee*; or
- the purpose for collecting or using the information is to recruit a potential employee.

An organization may disclose (section 21) personal employee information without consent when:

- the individual is an *employee* or was an employee; or
- the purpose for disclosing the information is to recruit a potential employee.

The collection, use and disclosure must be reasonable for the purpose, and the personal information must be limited to the work or volunteer work relationship. Before collecting the information about a current employee, the organization must advise the employee that it will collect the information and the purposes for the collection. If the information is about a *potential* employee (a job candidate), notification is not required.

For example, an organization might provide on-the-job training for its employees. The organization may collect test results for the participating employees without their consent, but must inform the employees of the intent to do this.

Organizations can also collect, use and disclose personal information of employees without consent under sections 14, 17, 20 or 22. Notice would not be required in this case.

EXAMPLE

Rob has applied for a job with ABC Inc. Rob's job application shows he recently worked for XYZ Enterprises. ABC Inc. can contact staff at XYZ Enterprises and collect personal employee information about Rob's time at XYZ, without Rob's consent. ABC can use the information as part of the hiring decision-making process; the information collected must be limited to what is reasonable to determine Rob's suitability for the job.

EXAMPLE

Rob has now been with ABC Inc. for three years and has applied for a different job within the company. Rob's main client is HJK Corporation and Rob spends half of his time at the HJK factory. ABC Inc. can contact staff at HJK Corporation for information about Rob's performance, if ABC Inc. notifies Rob in advance of the purposes for the collection. ABC can use the information as part of the competition decision-making process. The information can be retained as long as is reasonable for legal or business purposes.

EXAMPLE

Alice applied for a job with a photography company, Snapshots. Snapshots contacted Alice's former employer, Shutterbug, for a reference. Shutterbug disclosed more information than necessary when it provided detailed information about Alice's medical condition to Snapshots. Some limited medical information may have been required by Snapshots in order to accommodate Alice in the workplace; however, details such as a medical diagnosis are not reasonably related to the employment relationship, and cannot be collected or disclosed as part of an employment reference (see *PIPA Case Summary P2007-CS-003*).

For more information, see **Information Sheet 5: Personal Employee Information**, available at **pipa.alberta.ca**.

7 Follow special rules for business transactions

Bottom line: You may collect, use and disclose personal information without consent for "business transaction" purposes. Business transactions relate to a change in ownership of a business (section 22).

A ***business transaction*** includes the purchase, sale, lease, merger, amalgamation, acquisition or disposal of an organization, or part of an organization, or any business or activity or business asset of an organization. The transaction may include the taking of a security interest (for example, a mortgage) in the organization and includes a prospective transaction. This provision assists buyers of a business or part of a business to carry out due diligence research.

For a business transaction, an organization may collect, use and disclose personal information **without consent** if the organization:

- agrees to limit the collection, use or disclosure to purposes related to the transaction; and
- needs the information to decide whether to go ahead with the transaction.

If the transaction does not go ahead, the organization that collected the information for the transaction must return or destroy it.

This provision does not apply when purchasing, selling, leasing, transferring, disposing or disclosing personal information if this is the main purpose of the business transaction.

EXAMPLE

ABC Inc. is considering buying Rewind Enterprises, a video rental store. To decide whether to go ahead with the purchase, ABC wants to see some of Rewind's business records that contain personal information about customers and employees. Rewind may provide these records without consent of the individuals, as long as ABC has entered into an agreement to protect the information and not to use it for purposes other than its sale. If the deal goes through, ABC may continue to use the personal information for the original purposes for which it was collected. If the deal does not proceed, ABC must return the personal information to Rewind, or destroy it.

Follow the rules for giving access to, and correcting, personal information 8

Bottom line: You must give individuals access to their own information and respond openly, completely and accurately. There are a few exceptions to giving access.

An individual's general right of access to his or her information

An individual has the right to ask for access to his or her own personal information contained in a ***record*** that is in the ***custody*** or under the ***control*** of an organization (section 24).

An individual who makes a request for access is called an ***applicant***. A request by an applicant must give enough information so an organization that makes a reasonable effort can find the information. Normally requests would be made in writing. Organizations can choose to accept oral requests if the applicant is unable to put the request in writing. An applicant may ask to see the information or receive a copy of it. Applicants do not have to say why they are asking for the information.

The organization must respond to an applicant within 45 calendar days of receiving the request. Organizations may designate an office to receive requests, and the time limit for processing a request would not begin until the request arrived at a designated office. There are some situations in the Act that allow for a longer time period to respond to the request.

Unless it has no such record, or it can refuse access under the Act, an organization must:

- give the individual access to his or her personal information,
- tell the individual what the information has been or is being used for, and
- tell him or her to whom, and in what situations, the information is being or has been disclosed by the organization.

Organizations may not have a record of the persons or organizations that they have disclosed the individual's personal information to before January 2004. If this is the case, the organization should tell the individual to whom, or to what organization, it may have disclosed the information.

In dealing with an access request, the organization must act reasonably.

Can you charge fees?

You may charge an applicant a reasonable fee for access to the individual's personal information or to information about the use or disclosure of that information. However, organizations may not charge a fee for an access request made by an employee for employment information.

When charging fees, you must give the applicant a written estimate of the total fee for the service before you process the request. You may require the applicant to pay a deposit before processing the request. The records can be withheld from the applicant until any fees owing are paid by the applicant.

The 45-day clock for processing a request stops once an estimate is provided to the applicant. It does not start again until the estimate has been accepted, and the deposit received, if required. If the applicant has not responded within 30 days of when the estimate was given, then the organization can consider the request to have been withdrawn.

TIPS

- **A reasonable fee would include an amount to cover out-of-pocket costs, such as copying and postage.**
- **If the request involves only a few pages of records that are easy to locate, the fee should be minimal.**
- **If the request involves a large number of records, and it takes a long time to locate and produce the records, the fee could be larger.**

For more information on fees for access, see **PIPA Advisory 5 - Access Requests - Fees**, available at **www.oipc.ab.ca**.

Who can request personal information?

The individual that the information is about, or his or her *authorized representative*, may request access to the individual's personal information. Individuals may request records that contain personal information about them.

Who is an authorized representative?

An individual 18 years or older may do anything that the Act says the individual has a right or power to do, such as asking for his or her own personal information or giving consent. Minors can act on their own behalf if they understand their rights and powers, and the consequences of exercising them under the Act.

In some situations, an ***authorized representative*** may take the place of the individual. This means that another person has the authority to do what the individual can do under the Act. An authorized representative may be:

- a *guardian of a minor* (someone who makes day-to-day decisions affecting a minor, or who has care and control of the minor – this would often be a parent or a guardian appointed by the court)
- an executor or administrator of the estate of an individual who has died
- a guardian or trustee of a dependent adult
- an individual acting with the written authorization of an individual
- an individual who is acting under a power of attorney (section 61)

If an organization is in doubt concerning a person's authority to act on behalf of an individual, the organization may ask for a statutory declaration that states the grounds on which the person is authorized to act.

EXAMPLE

John Smith, the parent of Joey Smith, asks the For Kicks Soccer Club for access to his child's personal information. The child played with the Soccer Club for two years and is now 16 years old. He has not played with the club for several years.

Since Joey is a minor (under 18 years of age), the Club manager would have to decide if Joey can understand the right of access and the consequences of his father having access to his information. If the Club manager thinks that Joey would understand, then Joey should be the one who is asking for access to his own personal information. If the Club manager thinks that Joey will not be able to understand, then Mr. Smith could take Joey's place and ask for access to his son's personal information.

EXAMPLE

Carol recently died. She had worked at XYZ Company for 15 years. Her daughter Nancy has asked for a copy of her mother's personnel file to follow up on an insurance matter.

If Nancy can show XYZ Company that she is the executor or administrator of her mother's estate, then she can take the place of her mother and ask for access to her mother's file. But XYZ Company can only give Nancy the information that is needed to enable Nancy to administer her mother's estate.

How do you respond to a request for personal information?

An organization must make every reasonable effort to help applicants (***duty to assist***). Your response to an *applicant* must be open, complete and accurate (section 27). If the applicant asks, and if it is reasonable to do so, you must explain any term, code or abbreviation used in the record.

You must make a record of an *applicant's* personal information if the information is in electronic format and you can make the requested record using your normal computer equipment and programs, and if this would not unreasonably interfere with your operations (section 27(2)). For example, if you have a customer database and there is a report format for individual customers, or if you can print a screen view of the customer's personal information, then you must provide this information on request.

You can provide a copy of a *record* instead of allowing an individual to examine a record if:

- the records may be damaged, for example, if they are fragile historical documents,
- other information would be disclosed that is not permitted by the Act, such as personal information of another individual, or
- allowing inspection would unreasonably interfere with the operations of the organization, for example, an employee would have to supervise the inspection of documents for a significant amount of time while an applicant read them.

You must respond within 45 days of getting the request (section 28). The Act allows you to take an extra 30 days to respond if:

- the request does not give enough information to allow you to find the personal information or the *record* requested;
- a large amount of personal information is requested or has to be searched;
- completing the request in 45 days would unreasonably interfere with the operations of the organization; or
- you must consult with another organization or *public body* to decide if access should be given.

You may also ask the Information and Privacy Commissioner to authorize a longer period to respond (section 31(1)).

If you take extra time, you must tell the *applicant*:

- why you are taking more time,
- when you will respond to the request, and
- that he or she may make a complaint to the *Commissioner* about the organization taking more time to respond (section 31(2)).

If you do not respond to the applicant in the required time, an applicant may complain to the Information and Privacy Commissioner that your organization has refused access.

When you respond to a request, you must tell the *applicant*:

- whether you have a *record*;
- whether you will give access to all or part of the *record*; and
- where, when, and how access will be given, if it will be given.

If you refuse access to all or part of the record, you must tell the *applicant*:

- the reason(s) for refusing and the section(s) of the Act that allow, or require you, to refuse to give access;
- the name of the person in the organization who can answer questions about the refusal; and
- that he or she may ask the *Commissioner* to review the organization's decision to refuse access (section 29).

For more information on responding to a request, see **PIPA Advisory 3 - Access Requests - Responding to a Request**, available at **www.oipc.ab.ca**.

Exceptions to giving access

An organization can refuse access in a number of situations (section 24(2)). The ones most likely to come up are:

- when the information is protected by any legal privilege (for example, communications between a lawyer and a client when the client is asking for legal advice or the lawyer is giving legal advice to a client)
- when disclosure would give away confidential business information, and it is not unreasonable to hold back the information
- when the information was collected for an *investigation* or *legal proceeding*
- when disclosure might result in that type of information no longer being supplied and it is reasonable for the organization to need the type of information (for example, when a third party gives your organization an opinion about an individual, but would no longer give this kind of information if the individual were allowed to see the opinion)
- when a mediator or arbitrator collected the information

When an organization has decided to refuse access to some records, the personal information in the remaining records must be provided to the applicant.

EXAMPLE

Joe, a former employee of ABC Corporation, asked for access to his personnel file. Joe and ABC Corporation were involved in a dispute before the Appeals Commission for Alberta Workers' Compensation. ABC Corporation reviewed Joe's file and refused to give him access to the following personal information on his file:

- **information prepared by company lawyers about the Workers' Compensation dispute and the grievance filed by Joe (information protected by legal privilege); and**
- **information about ABC Corporation's investigation into Joe's fitness to work (information collected for the investigation).**

An organization must refuse access if disclosure:

- could reasonably be expected to threaten the life or security of another individual;
- would show personal information about another individual; or
- would identify the individual who gave you an opinion about someone else in confidence and the individual giving the opinion does not consent to the disclosure of his or her identity. You can hold back the identity of the person who wrote the opinion while still giving access to the opinion itself, unless the applicant could figure out who gave the opinion by reading it (section 24(3)).

If any of the information in a record meets these criteria, that information should be withheld. The remaining information would then be given to the individual (section 24(4)).

EXAMPLE

Mary applies for a promotion in her company. Three employees of the company are asked by a human resources consultant to give their opinions about Mary's work habits and leadership ability. The human resources consultant makes notes of their comments on the competition file. After Mary does not get the promotion, she asks for access to her file, including the notes made by the human resources consultant.

The company reviews Mary's file and asks the employees if they will consent to the release of their names. One employee gives her consent but two employees, who have had an ongoing feud with Mary, do not give their consent. The company gives Mary partial access to her file, including the comments of the three employees and the name of the one employee who consented to the release of her identity. The company removes the names of the two employees who did not give consent. Also removed was information that would reveal the identity of each of the individuals who gave opinions about Mary and did not consent to disclosing his or her identity.

EXAMPLE

Bill's loan application was rejected by his credit union. He made a request to the credit union for the records containing his own personal information for the last five years. Bill was divorced two years ago. In providing the records to Bill, the credit union would need to remove any personal information about his ex-wife, or any other individual, which may appear in the records.

TIPS

- **Try to keep personal information about an individual in one place to make finding it for an access request easier. Alternatively, keep a record of where all such information can be found.**
- **Never disclose personal information unless you are sure of the identity of the applicant and of the applicant's right of access.**

For more information on exceptions to access, see **PIPA Advisory 7 - Access Requests - Exceptions to Access**, available at **www.oipc.ab.ca**.

Requests for corrections to personal information

An individual who believes that his or her personal information under the *control* of an organization has a mistake in it, or is missing some information, may ask the organization to correct it (section 25).

A request for correction must give enough information so an organization that makes a reasonable effort can find the information. Normally requests would be made in writing. Organizations can choose to accept oral requests if the *applicant* is unable to put his or her request in writing. You cannot charge a fee for handling requests for correction.

How to respond to a request for correction

It is up to your organization to decide if you should correct the information. If you decide the information should be corrected, then it must be done as soon as possible. If it is reasonable to do so, the organization must send corrected information to every organization that it disclosed the wrong information to.

If the organization decides not to make a correction, it must make a note on the personal information saying that a correction was requested.

When an organization gets a notice that another organization has corrected an individual's personal information, the organization getting the notice must also correct any personal information about the individual that is in its *custody* or under its *control*.

An organization must not correct or change an opinion, including an opinion from a professional (for example, a doctor) or an expert. Opinions about an individual are based on the other person's view at the time the opinion was given. It may be important to have a record of that view later (section 25(5)).

EXAMPLE

Joy recently discovered that XYZ Company's records indicate that she is married. She sends a request for correction to show her status as single. XYZ should correct their records, and, if they have disclosed that information, notify other organizations that received it.

EXAMPLE

Randy recently returned to work after a few weeks off with a broken leg. The company doctor sent a note to his supervisor saying that Randy should not have to stand for more than three hours a day. Randy was copied on the note. Randy went to his own doctor who advised that he should not stand for more than one hour a day. Randy asked the company to change the opinion on file. The company cannot correct a professional opinion, but can add Randy's request to make the correction to the file.

For more information on requests for corrections, see **PIPA Advisory 4 - Requests for Correction of Personal Information**, available at **www.oipc.ab.ca**.

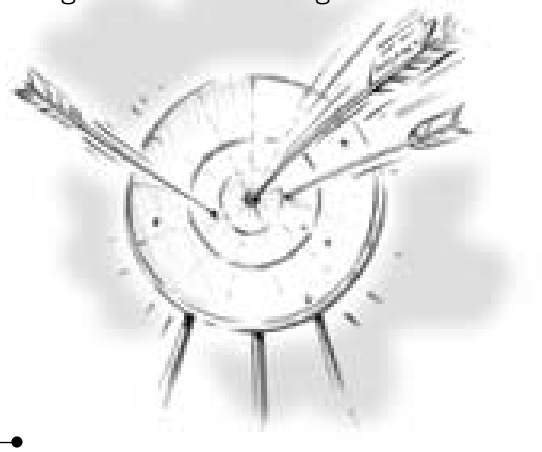
9 Follow the rules for accuracy, protection and retention of personal information

Bottom line: Take care of records that you create or receive and keep. Ensure they are accurate, appropriately protected and retained for reasonable purposes.

Accuracy

You must take reasonable steps to make sure that personal information collected, used or disclosed by your organization is **accurate** and **complete**.

This doesn't mean that you must routinely update all information. Just update it to the extent reasonable for its use. This rule helps to prevent using inaccurate or wrong information to make a decision about an individual.



What is reasonable depends on the circumstances. For example, be careful when you get personal information from someone other than the individual. The information may not be correct, or you may not have "the whole story." Also, what is reasonable will depend on what the information is going to be used for and how that will affect the individual.

Protection

You must use reasonable **safeguards** (physical, administrative and technical) to protect personal information from such actions as:

- someone getting access to, or collecting, using, copying or disclosing, personal information when he or she is not supposed to;
- someone misusing, stealing or losing personal information; or
- someone collecting, using, disclosing, copying, changing, destroying or not properly getting rid of, personal information.

Safeguards should be appropriate to the sensitivity of the information.

Examples of physical safeguards include:

- locking file cabinets and areas where files are stored when no one is there
- allowing only employees who need access to the storage areas or filing cabinets to have access to them
- clearing files and records containing personal information off your desk at the end of the day
- shredding papers containing personal information rather than placing them in a garbage can or recycling bin (see *IPC Investigation Report P2005-IR-001*)

Examples of administrative safeguards include:

- training employees so they know your policies or rules for protecting personal information and the consequences of not following them
- ensuring that personal information, especially sensitive information, is accessible only to those employees who need to know the information
- only storing as much personal information as is necessary on mobile devices such as laptops and USB flash drives (see *IPC Investigation Report P2006-IR-005*)
- using cover sheets when faxing personal information, and establishing procedures for ensuring only the authorized recipient has received the fax, especially when the personal information is sensitive (see *IPC Investigation Report P2005-IR-006*)
- having employees take an oath of confidentiality
- conducting audits to ensure employee compliance with safeguard procedures

Examples of technical safeguards include:

- using equipment or software that truncates debit and credit card numbers on receipts
- using password-protected screensavers so visitors cannot see information on computers
- using firewalls and anti-virus programs on computers
- using passwords to make sure that only certain workers have access to information on computers and changing the passwords often
- encrypting mobile electronic devices containing personal information, such as laptops and USB flash drives (see *IPC Investigation Report P2006-IR-005*)
- erasing computer hard drives before you sell or donate them

For more information on safeguards for protecting privacy, see **PIPA Advisory 8 - Reasonable Safeguards**, available at **www.oipc.ab.ca**.

For more information on safeguards for retail businesses, see **Privacy Proofing Your Retail Business**, available at **www.oipc.ab.ca.**

Retention

Keep personal information only as long as it is reasonable to carry out business or legal purposes.

Organizations may already have their own approved retention periods or schedules for records based on financial, legal, operational, audit or *archival* requirements. These retention periods should be followed.

Note that even if an individual has changed or withdrawn his or her consent for collecting, using or disclosing information, an organization can keep that information if there are legal or business reasons to do so.

Use care in disposing of or destroying personal information to prevent unauthorized parties from gaining access to the information.

How will the Act be enforced?

The Commissioner can investigate complaints and hold inquiries

The Information and Privacy Commissioner is the same ***Commissioner*** as under the *Freedom of Information and Protection of Privacy Act* and the *Health Information Act*. He has the power to review the actions and decisions of organizations under PIPA. For example, the *Commissioner* can review or investigate:

- any decision, action or failure to act by an organization that has been asked to give access to or to correct personal information (section 46(1));
- a claim by an individual that his or her personal information has been improperly collected, used or disclosed (section 36(2)); or
- a complaint about an organization not properly helping an applicant, about the time taken to respond to a request, or about the fees charged (section 36(2)).

The *Commissioner* can:

- send the individual to another grievance, complaint or review process (for example, the organization or its industry association may have its own complaint resolution process) (section 46(3));
- try to settle a complaint using mediation (section 49);
- hold an inquiry (section 50), including joint inquiries with privacy commissioners in other jurisdictions;
- issue Orders that are binding (section 53 and section 52(6));
- give an advance ruling on a matter that could be investigated under the Act (section 36(3)); and
- allow an organization not to respond to requests, or to take more time to respond in certain situations (section 37).

For more information on the role of the Commissioner's Office, see **A PIPA Guide for Organizations: Understanding the Role of the OIPC**, available at **www.oipc.ab.ca**.

Duty to comply with Commissioner's Orders

The organization must comply with a Commissioner's Order not later than 50 days from the day the Order is given to the organization. The exception is when an organization or individual applies for judicial review of a Commissioner's Order. For example, this might happen if the organization or individual feels the inquiry process was unfair or biased or that the *Commissioner* made an error in law. The individual or organization must apply for judicial review not later than 45 days from the day that the person applying is given a copy of the Order. The Commissioner's Order is then stayed until the Court of Queen's Bench deals with the application.

EXAMPLE

A customer purchases several books from her local bookstore, using her credit card. The customer notices that her credit card number appears in full on her receipt, along with the expiration date. The customer also notices the sales clerk keeps store copies of the receipts in an open tray beside the cash register. The customer is concerned that an unscrupulous patron of the bookstore could easily slip some receipts into a pocket and use the information for fraudulent purposes. The customer takes her concerns to the Commissioner's Office.

Before the Commissioner's Office opens a file, they will ask the customer if she tried to resolve her complaint with the bookstore. If she has not, she may be asked to do that. If she has, the Commissioner's Office will open a file on the complaint. Someone from the Office will contact the customer and the bookstore and try to help them work things out between them. If this cannot be done, the Commissioner may hold an inquiry. Most complaints are resolved without an inquiry. An inquiry can be done in writing or in person. The Commissioner must issue an Order following an inquiry.

An organization is protected from liability

An organization and a person involved in the administration of the Act are protected from liability for damages, if the organization or person has acted in good faith when disclosing or withholding information in accordance with the Act, or failing to give a required notice where reasonable care was taken (section 57).

In addition, organizations and individuals cannot be prosecuted for an offence under any statute if they are following a Commissioner's Order (section 59(3)), or be found guilty of an offence under this Act if they acted reasonably (section 59(4)).

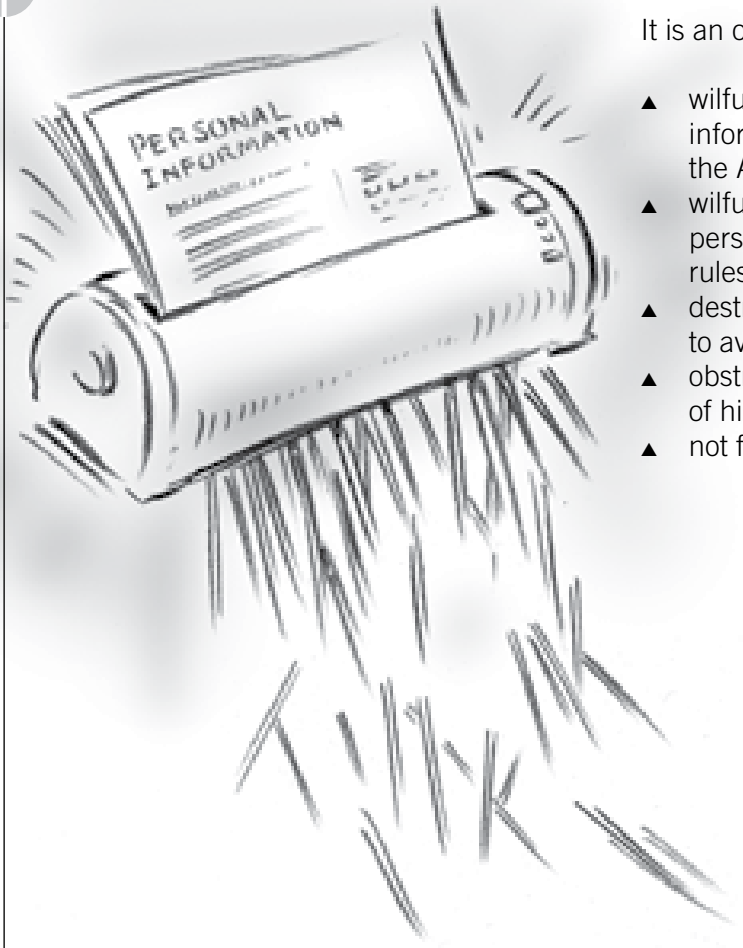
An employee can blow the whistle on an organization

An employee, acting in good faith, can tell the *Commissioner* about a situation he or she reasonably believes to be a contravention of the Act. The employee can also refuse to do something he or she believes is contrary to the Act.

The *Commissioner* will then investigate the claim. The "whistleblower" is protected from the organization taking any negative action such as firing or suspending the employee.

An employee of an organization, acting in good faith, is also protected from any negative action by the organization if the employee does something to avoid breaking the law (breaching PIPA) (section 58).

A person can be convicted of an offence under the Act



It is an offence under the Act to:

- wilfully collect, use or disclose personal information in a way that breaks the rules in the Act;
- wilfully try to obtain or obtain access to personal information in a way that breaks the rules in the Act;
- destroy, hide or change personal information to avoid dealing with an access request;
- obstruct or mislead the *Commissioner* or one of his staff; or
- not follow a Commissioner's Order.

An act is done **wilfully** if done voluntarily and intentionally, and with the specific intent to do something the law forbids.

If you are convicted of an offence, fines are up to $10,000 for individuals and up to $100,000 for organizations.

Note that acting in good faith (acting honestly and reasonably) protects both individuals and organizations from legal actions. If they act in good faith to disclose, or not to disclose, part of a record or personal information that causes loss or injury to someone, they cannot be personally sued (section 57).

An individual can sue for damages for breach of the Act

An individual can sue an organization for damages for loss or injury when an organization has failed to meet its obligations under the Act. This could happen after the *Commissioner* has made an Order that finds the organization has contravened PIPA or after the organization has been convicted of an offence under the Act. An individual affected by the Order, or by the action that resulted in the offence, can sue for damages for loss or injury (section 60).

Definitions of terms used in this guide

Applicant means an individual who requests access to personal information or for a correction of personal information.

Archival institution means an institution to which archival records are transferred for permanent preservation and that provides public access to its collection.

Archival purposes means for the purposes of preserving archival records and making those records available to the public in an archival institution.

Archival records means records of historical or archival importance.

Authorized representative means a person who is authorized to exercise any right or power under the Act on behalf of an individual, such as the right to request access or the power to consent. Some authorized representatives are:

- a guardian of an individual under 18 years of age
- the personal representative of an individual who has died, if the right or power relates to administering the individual's estate
- a guardian or trustee appointed under the *Dependent Adults Act*
- an individual acting under a power of attorney (section 61)

Business contact information means an individual's name and position name or title, business telephone number, business address, business e-mail, business fax number and similar business information (section 1(a)).

Business transaction means a transaction consisting of the purchase, sale, lease, merger or amalgamation or any other type of acquisition or disposal of, or, the taking of a security interest in respect of, an organization or a portion of an organization or any business or activity or business asset of an organization and includes a prospective transaction of this nature (section 22(1)(a)).

Commercial activity means any transaction, act or conduct, or any regular course of conduct that is of a commercial character and includes the following:

- selling, bartering, or leasing of membership lists or of donor or other fund-raising lists,
- operating a private school or an early childhood services program as defined in the *School Act*, or
- operating a private college as defined in the *Post-secondary Learning Act* (section 56(1)(a)).

Commissioner means the Information and Privacy Commissioner appointed under the *Freedom of Information and Protection of Privacy Act* (section 1(b)).

Control of personal information by an organization means an organization's decision-making power on how to use, disclose and store personal information, how long to keep it and how to dispose of it. For example, personal information in the custody of a contractor providing services to the organization is still under the control of the organization through the terms of its contract with the service provider.

Custody of personal information means the keeping of personal information by an organization in its offices, facilities, file cabinets, computers, etc.

Disclosing personal information means showing, sending, telling or giving a person or some other organization personal information that is in the custody of the organization.

Domestic means related to home or family (section 1(d)).

Duty to assist means the Act's requirement to make every reasonable effort to respond to an access request openly, accurately, and completely, and within the time limits under the Act.

Employee means an individual employed by an organization and includes an individual who performs a service for, or in relation to, an organization
- as an apprentice, volunteer, participant or student, or
- under a contract or an agency relationship with the organization (section 1(e)).

FOIP Act means the *Freedom of Information and Protection of Privacy Act*, the Act that governs access to information and protection of privacy of personal information in the Alberta public sector.

Guardian of a minor means someone who is legally responsible for an individual under the age of 18 years.

Investigation means an investigation related to:
- a breach of an agreement,
- a contravention of an enactment of Alberta or Canada or of another province of Canada, or
- circumstances or conduct that may result in a remedy being available at law, if the breach, contravention, circumstances or conduct in question has or may have occurred or is likely to occur and it is reasonable to conduct an investigation (section 1(f)).

Legal proceeding means a civil, criminal or administrative proceeding related to
- a breach of an agreement,
- a contravention of an enactment of Alberta or Canada or of another province of Canada, or
- a remedy available at law (section 1(g))

Local government body means a local government body as defined in the *Freedom of Information and Protection of Privacy Act* (section 1(i)) such as a municipality, a Métis settlement, a housing management body, an irrigation district, a public library, or a police service or commission.

Local public body means a local public body as defined in the *Freedom of Information and Protection of Privacy Act* (section 1(j)) such as a local government body, a regional health authority, a public school board or a public post-secondary educational institution.

Managing personnel means the carrying out of that part of human resource management relating to the duties and responsibilities of employees. It can also refer to administering personnel and includes activities such as payroll and succession planning (PIPA Regulation AR 366/2003, section 3).

Non-profit organization means an organization that is incorporated under the *Societies Act* or the *Agricultural Societies Act* or that is registered under Part 9 of the *Companies Act* or that meets the criteria that may be established under the regulations to qualify as a non-profit organization (section 56(1)(b)).

Organization includes:
- a corporation,
- an unincorporated association,
- a trade union as defined in the *Labour Relations Code*,
- a partnership as defined in the *Partnership Act*, or
- an individual carrying out a business (section 1(i)).

Personal employee information means information about an individual employee or potential employee that is reasonably required by an organization and is collected, used or disclosed solely to establish, manage or terminate:
- an employment relationship, or
- a volunteer work relationship

between the organization and the individual. It does not include personal information about the individual that is unrelated to those relationships (section 1(j)).

Personal information means information about an identifiable individual (section 1(k)).

PIPA means the *Alberta Personal Information Protection Act*.

PIPEDA means the federal *Personal Information Protection and Electronic Documents Act*.

Professional regulatory organization means an organization incorporated under a professional Act that regulates a professional or occupational group or discipline (section 55(1)(d)).

Public body means a public body as defined in section 1(p) of the *Freedom of Information and Protection of Privacy Act* such as a government department, a regional health authority, a municipality, a public school board or public post-secondary educational institution.

Publicly available information means for the purposes of section 14(e), 17(e) and 20(j) of the Act:

- personal information – name, address, telephone number – contained in a telephone directory that is available to the public where the individual can refuse to have the information appear in a directory.
- personal information – including the name, address, telephone number, e-mail address – contained in a professional or business directory, listing or notice that is available to the public, where the collection, use or disclosure of the personal information relates directly to the purpose for which the information appears in the directory.
- personal information contained in a government registry to which the public has access – including Land Titles, Personal Property Registry, Corporate Registry – where the collection, use or disclosure of the personal information relates directly to the purpose for which the information appears in the registry.
- personal information contained in a registry operated by an organization or a local public body under a statute and to which the public has access, where the collection, use or disclosure of the personal information relates directly to the purpose for which the information appears in the registry.
- personal information contained in a record of a quasi-judicial body that is available to the public where the collection, use or disclosure of the personal information relates directly to the purpose for which the information appears in the record.
- personal information contained in a publication – including a magazine, book, or newspaper, whether printed or electronic – available to the public and it is reasonable to assume that the individual that the information is about provided the information.
- personal information collected in similar circumstances from outside of Alberta (PIPA Regulation AR 366/2003, section 7).

Reasonable means what a reasonable person would think was appropriate in the circumstances (section 2).

Record means a record of information in any form or in any medium, whether in written, printed, photographic or electronic form or in any other form, but does not include a computer program or other mechanism that can produce a record (section 1(m)).

Using personal information means using it to carry out a purpose of the organization such as providing a product or service or assessing whether an individual is eligible for a benefit. Using personal information includes copying or reproducing the information.

Notes

pipa Personal Information Protection Act

Alberta

Access and Privacy
Service Alberta
3rd Floor, 10155 – 102 Street
Edmonton, Alberta T5J 4L4
Phone: 780-644-PIPA (7472)
Toll free dial 310-0000 first
E-mail: **pspinfo@gov.ab.ca**
Website: **pipa.alberta.ca**

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