

## GENERAL

### 1. What is the purpose of the Personal Information Protection Act (PIPA)?

The purpose of the Act is to govern the collection, use and disclosure of personal information by organizations, in a manner that recognizes both the right of an individual to have his or her personal information protected and the needs of organizations to collect, use and disclose personal information for purposes that are reasonable (section 3).

### 2. Why did Alberta enact legislation to protect personal information held by the private sector?

Private sector privacy legislation has become increasingly important to individuals and organizations in the last two decades, largely as a result of advances in information technology that allow organizations to store and manipulate large amounts of personal information. This has led to pressure on governments everywhere to regulate the collection, use and disclosure of personal information in the private sector, as it already does in the public sector. It has also led to the recognition by business of the importance of privacy protection as a competitive business value, especially in electronic commerce.

### 3. When did Alberta's Act come into effect?

Alberta's *Personal Information Protection Act* and regulation came into effect on January 1, 2004. It was declared substantially similar to PIPEDA on October 12, 2004.

### 4. What are some of the Act's requirements?

Some of the Act's requirements are:

- Organizations may collect personal information only to the extent that is reasonable for meeting the purposes for which the information is collected.
- Organizations may use or disclose personal information only for the purposes the information was originally collected, except with the consent of the individual or as permitted by the law.
- When an organization collects personal information from an individual, it must give notice of the purpose of collection and a contact for questions.
- Organizations must make a reasonable effort to ensure that any personal information it collects, uses, or discloses is accurate and complete.
- Organizations must make reasonable security arrangements to protect personal information against security risks.
- Organizations must notify the Information and Privacy Commissioner if an incident occurs that involves loss of or unauthorized access to or disclosure of personal information that may pose a real risk of significant harm to individuals.
- Organizations must provide an individual with access to his or her own personal information, and allow for corrections to that information, as long as the request is reasonable and exceptions do not exist that prevent access or corrections. The organization may charge reasonable fees for providing access.

- An organization is responsible for the personal information in its custody or under its control and must designate one or more individuals who are responsible for ensuring the organization complies with the Act.

## PIPEDA

### 5. What is PIPEDA?

PIPEDA stands for the *Personal Information Protection and Electronic Documents Act*. This is a federal act that specifies how private sector organizations may collect, use or disclose personal information in the course of commercial activities.

Federally regulated businesses operating in Alberta, such as banks and telephone companies, are governed by PIPEDA. PIPEDA applies when Alberta organizations carry out business (involving personal information) across provincial borders.

### 6. Do other provinces have private sector privacy legislation?

Quebec has had private sector privacy legislation in place since 1994. British Columbia's *Personal Information Protection Act* came into effect on January 1, 2004. PIPEDA applies in all other provinces.

## PERSONAL INFORMATION

### 7. What personal information is covered by PIPA?

Personal information is defined in section 1(k) as information about an identifiable individual. The information may be recorded or not. For example, it includes:

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

Business contact information is personal information. It includes information normally found on a business card, such as job titles, business telephone numbers (office, cell or fax), business address and e-mail address. PIPA does not apply to business contact information that is collected, used or disclosed solely for the purposes of enabling the individual to be contacted in relation to the individual's business responsibilities (section 4(3)(d)).

## SCOPE

### 8. How are public bodies under the *Freedom of Information and Protection of Privacy Act (FOIP Act)* affected?

PIPA does not apply to public bodies, or to personal information in the custody of an organization if the FOIP Act applies to the personal information (sections 4(2) and 4(3)(e)).

### 9. Does the Act apply to health information?

PIPA applies to medical information held by private-sector organizations, such as information in an employee's personnel record about a workplace injury. However, the Act does not apply to "health information," as defined in the *Health Information Act*, in the custody or under the control of a "custodian" (e.g., a pharmacy).

### **10. When does an organization need consent to collect, use or disclose personal information?**

Consent is normally required. Consent may be provided orally or in writing (including electronically), or it could be implied if an individual provides his or her information to the organization voluntarily. The Act provides for implied and opt-out consent. Personal information should be collected directly from the individual, unless the individual provides consent for collection from other sources. An organization cannot, as a condition of providing a service, require an individual to consent to the collection, use or disclosure of information beyond what is necessary to provide the service (sections 7 and 8).

### **11. When can opt-out consent be used?**

The Act allows organizations to rely on opt-out consent in some circumstances, taking into account the sensitivity of the information. Organizations will need to notify the individual of the purposes for which the information is being collected, used and disclosed, and to allow the individual a reasonable period of time to decline or object to the proposed collection, use or disclosure (section 8(3)).

### **12. When is consent not needed?**

The Act permits the collection, use and disclosure of personal information without consent in specific and limited circumstances. For example, personal information can be collected without consent if the collection is required by law, for an investigation, legal proceeding or to collect a debt, or if the personal information is publicly available, as defined in the regulation (Part 2). An example of when consent is not required to disclose personal information is if the disclosure is necessary to respond to an emergency (section 20(g)). Employee information can be collected, used and disclosed without consent in some circumstances (sections 15, 18, and 21). Consent is not needed to collect, use or disclose business contact information, as long as the information is used to contact the individual in relation to the individual's business responsibilities and for no other purpose (section 4(3)(d)).

### **13. What happens if a business needs to disclose personal information to a potential purchaser of the business?**

The Act allows an organization to disclose personal information to a prospective purchaser without consent if the information is necessary to determine whether the prospective purchaser would want to buy the business. The prospective purchaser will be required to safeguard the information and will not be permitted to retain or use the information for other purposes. (section 22)

### **14. Does an organization need to go back and get consent to use personal information collected before January 1, 2004?**

Such personal information may continue be used for the purposes for which the information was collected. The Act deems that consent was provided for the collection of the information, and it can be used and disclosed for purposes for which it was collected. Once the Act came into force, it is treated the same as information collected after January 1, 2004.

Organizations need to ensure they only use and disclose personal information they already hold in accordance with the Act. Organizations should build a consent process into their regular contact with customers so that customers are aware of the purposes for collecting the information.

Information can be used and disclosed only for purposes that are reasonable. Also, the information may be used or disclosed only to the extent that is reasonable for meeting the purposes of the use or disclosure. This means that personal information that was collected before 2004 may not be used or disclosed for unreasonable purposes or in excess of what would be necessary for the purpose. It should not be used if the organization would not be permitted to collect it after January 2004.

For example, if an individual provided his name and mailing address in order to receive a catalogue, the business may continue to use that information to send out catalogues. If the business had collected the individual's drivers license number to use as an identifier, the number could not be used for that purpose after January 2004 without consent. If the business wants to use the contact information for a new purpose, then a new consent will be required (section 4(4)).

**15. A retailer has a database of customer personal information collected in relation to warranties for products purchased from the retailer. Prior to January 1, 2004, the retailer used the customer information for servicing the products and sending promotional material to the customers. Can the retailer continue to use the customer information for these purposes?**

The Act permits an organization to use personal information collected prior to January 1, 2004 for the purposes for which it was originally collected.

The retailer can continue to use the customers' personal information for servicing the warranties as this is clearly the purpose for which the information was originally collected.

In deciding whether it would be reasonable to continue to use the customers' information for promotional or marketing purposes, the retailer should consider the reasonable expectations of the customer at the time he or she provided the information to the retailer. If at the time of collecting the personal information the retailer specified that it uses personal information for marketing purposes, it would be reasonable for the retailer to continue to use the customer information for this purpose. If the customer answered questions contained on the warranty registration card about other products used by the customer, it may be reasonable for the retailer to use the information for sending promotional material about other products to the customer.

When it is unclear what the reasonable expectations of the customers were, the best practice is for the retailer to seek the consent of the customers to use their personal information for promotional or marketing purposes. During the next regular communication with its customers, the retailer can provide the customers with an opportunity to opt-out of having their information used for promotional or marketing purposes. For those customers that indicate they do not want their personal information used for these purposes, the retailer must use the information only for servicing the warranty.

**16. The retailer also disclosed the customers' names and addresses to another business that sells complementary products or services. Can the retailer continue to disclose the customers' personal information for this purpose?**

Again, the reasonable expectations of the customers at the time their personal information was collected should be considered. If there was a reasonable expectation on the part of the customers that their personal information would be passed on to the other business, the retailer could continue to disclose the customers' personal information for this purpose. If the customers were unaware of the disclosure, it would not be reasonable for the retailer to continue to disclose the customers' personal information to another business. The retailer would need to obtain the consent of customers to do this.

**17. How long can an organization keep the personal information it collected about an individual prior to January 1, 2004?**

The Act requires an organization to retain personal information only as long as the organization reasonably needs the information for business or legal purposes.

An organization can keep the information it reasonably needs to continue to fulfill the purposes for which the information was originally collected or for other purposes to which the individual has consented. If the organization collected more personal information than it needs to fulfill those purposes, it must dispose of the information no longer needed in a safe manner, or delete the identifiers (e.g. names and account numbers).

An organization may also keep personal information for legal purposes. This includes any contractual obligation or any statutory requirement (e.g. the *Income Tax Act*) that requires the information to be retained for a certain period of time. An organization may also need to keep personal information for a legal proceeding it is involved in or has a reasonable expectation of being involved in (e.g. a customer is suing a retailer for failing to fulfill its warranty obligations).

When an organization no longer needs the personal information for business or legal purposes, it must destroy the information in a secure manner or anonymize the information.

**18. Can an individual request to see the personal information an organization collected about him or her prior to January 1, 2004?**

Yes. The Act gives an individual the right of access to his or her own personal information contained in a record in the custody or under the control of an organization, subject to certain exceptions. In addition to requesting to see the original records or a copy of them, the individual may also enquire about the purposes for which the organization has used and is using the information and to whom and for what purposes the information has been or is being disclosed.

An organization may not have complete records of how it used or to whom it disclosed personal information before January 1, 2004. In such cases, it would be reasonable for the organization to state the purposes the information may have been used for and to whom and for what purposes it may have been disclosed.

In certain instances, the Act permits or requires an organization to refuse an individual access to personal information (e.g. the information is protected by solicitor-client privilege, the information would reveal personal information about another individual, or the information was collected for an investigation or legal proceeding).

A right of access applies only to personal information that is in the custody or under the control of the organization at the time of the request (e.g. it does not apply to personal information that was destroyed by the organization before January 1, 2004).

**19. Can an individual tell an organization to no longer use or disclose the personal information it collected about the individual prior to January 1, 2004?**

Yes. The Act allows an individual to withdraw or vary consent to the collection, use or disclosure of personal information by an organization, regardless of when the information was collected.

The individual must give the organization reasonable notice that consent is being withdrawn or varied. The organization must inform the individual of the likely consequences of the consent being withdrawn or varied, if the consequences are not reasonably obvious to the individual.

The organization must stop collecting, using or disclosing the personal information when consent is withdrawn or abide by the varied consent except:

- a) where the Act permits an organization to collect, use or disclose personal information without consent, or
- b) where the withdrawal or variation of consent would frustrate a legal promise or duty owed by either the organization or the individual (unless the parties otherwise agree).

**“REASONABLE PERSON” TEST**

**20. How is the “reasonable person” test used in PIPA?**

The Act uses a test of what is reasonable throughout. The Act doesn't set out steps the organization must follow in all circumstances.

The reasonable person test is an objective legal test. Reasonable judgment is not what you or I may think is reasonable. It is the judgment of an objective third party.

An organization needs to be able to demonstrate that it considered the circumstances around handling personal information and made a decision on what is reasonable in the circumstances.

## WORKPLACE

### 21. How does the Alberta Act apply to the workplace?

The Act covers employment information. The definition of employee includes partners, directors, officers, apprentices, volunteers, participants, students, and individuals under contract to an organization (section 1(1)(e)). Employees have a right of access to their own information (section 24). They will also have the ability to request correction of erroneous information (section 25). Employers are able to collect, use and disclose certain employee information without consent when it is reasonable to do so, for example, in relation to a recruitment process (sections 15, 18 and 21).

### 22. Can I disclose an employee's home phone number without consent because it is listed in the telephone book?

No. A home telephone number is the personal information of the employee. Under section 7(a) of the PIPA Regulation, personal information is publicly available if it is contained in a telephone directory (additional conditions apply). The provision in section 20(j) to disclose publicly available information without consent applies only when an organization is collecting, using, or disclosing information **directly from** the telephone directory. It does not apply to disclosing telephone numbers from the organization's records.

### 23. Can an employee ask to see his or her personnel file?

Yes. An employee can request access to any personal information about them. This includes their personnel records, including any "unofficial" files that may be held by supervisors (section 24). The organization has 45 calendar days to provide access (section 28). Some personal information may be withheld from an employee under limited and specific circumstances set out in section 24. For example, the identity of an individual who provided an opinion in confidence must be withheld if the individual who provided the opinion does not consent to being identified. The organization cannot charge a fee to process a request for personal employee information (section 32(1.1)).

Organizations processing requests for personal information should be careful to consider what is the personal information of an employee – it must be personal information "about" the individual and is not necessarily each record containing the employee's name. For example, each letter signed by an employee in the course of their duties is not likely to be "personal information" of that employee.

Employers do not need to limit access to requests made under the Act to make this information available. The information can continue to be provided under company policy, but employees can make a written request under the Act if the company refuses to provide access to the records or withholds information.

### 24. When can an organization provide a reference?

An organization can provide a reference for a current or former employee, without consent, to a potential or current employer (section 21(2)). An "employee" includes a partner, director, officer, apprentice, volunteer, participant, work experience student or an individual under contract (section 1(1)(e)).

The information disclosed must be limited to information that was collected by the organization as personal employee information, i.e. information that was reasonably required by the organization to establish, manage or terminate its relationship with the employee (section 1(l)(j)). In addition, it must be reasonable to disclose the information for the purpose of assisting the potential or current employer to determine the employee's eligibility or suitability for a position with that

employer (section 21(2)). The organization must also make a reasonable effort to ensure that the personal information provided in a reference is accurate and complete (section 33).

**25. Some organizations have a policy that they will provide a reference only with the consent of the individual the reference is about. Can organizations require consent to provide a reference?**

Yes. PIPA permits, but does not require, an organization to provide an employment reference without consent. An organization can establish a policy that it will give a reference only with the consent of the individual the reference is about. An example of a consent form that permits an organization to disclose personal information for the purposes of a reference is located at the end of these questions.

An organization giving a reference with consent must still disclose only the type and amount of personal information about the employee that is reasonable to fulfill the purpose of the reference (section 19). The organization must also make a reasonable effort to ensure that the personal information disclosed is accurate and complete (section 33).

**26. A job candidate did not list an employer as a referee. Can the organization considering the candidate for a position contact the employer for a reference?**

Yes. PIPA allows an organization to collect, without consent, a reference about a job candidate (section 15(1)). The Act does not require the candidate to name the organization as a referee. Nevertheless, it is always a good practice for the organization to first discuss with the candidate why the employer was not listed as a referee.

Organizations can also establish the stricter standard of collecting a reference only with the consent of the job candidate. An example of a consent form that permits an organization to collect personal information for the purposes of a reference is located at the end of these questions.

Any personal information collected in a reference, whether with or without consent, must be limited to information that is reasonably required to determine the candidate's eligibility or suitability for the position (sections 11 and 15(1)(b)) and must be as accurate and complete as reasonably possible (section 33).

**27. Can an individual ask an organization to see a reference that has been given?**

The Act gives an individual the right to request access to his or her own personal information that is contained in a record in the custody of or under the control of an organization (section 24(1)). The Act also requires an organization to provide information about how the individual's personal information has been or is being used, and inform the individual of the names of the persons to whom the information was disclosed and the purposes for which the information was disclosed (section 24(1)(1.2)).

With respect to a reference, an individual can request access from either the organization giving the reference or the organization collecting the reference. Since an organization is required to provide access only to recorded personal information (section 24(1.1)), the right of access would not extend to a reference given verbally. However, the individual could request access to any notes made about the reference by either the organization collecting the reference or the organization giving the reference.

There are certain circumstances where the Act allows an organization to refuse access to records. For example, the organization collecting the reference **may** refuse to grant access to the recorded information if it might result in references in general no longer being provided to the organization (section 24(2)(d)).

In other circumstances, the Act requires an organization to refuse access to records. The organization collecting the reference and the organization providing the reference **must** refuse access if, for example

- the information would reveal personal information about another individual (section 24(3)(b)), or
- the information would reveal the identity of an individual who has given an opinion in confidence and who does not consent to having his or her identity revealed (section 24(3)(c)).

If the personal information about another individual or the identity of the individual who gave the opinion can be reasonably severed from the record, the organization must provide access to the remainder of the record (section 24(4)).

A person's opinion about another individual is the personal information of the individual the opinion is about. It is not the personal information of the person who gave the opinion. However, the opinion may contain information that would reveal the identity of the person who gave the opinion. If the person who gave the opinion does not consent to his or her identity being revealed, the Act requires the identifying information to be severed before access to the opinion is given to the individual the opinion is about. If the identifying information cannot be severed, the organization must refuse access to the entire opinion.

**28. What can an individual do if an organization discloses inaccurate personal information in a reference?**

PIPA requires an organization to make a reasonable effort to ensure that personal information that is being collected or disclosed in a reference is accurate and complete to the extent that is reasonable for the purpose for which the information is being collected or disclosed (section 33).

If an individual believes an error or omission has occurred, the individual may make a request for a correction to the organization collecting the reference and to the organization providing the reference (section 25(1)).

If the organization decides a correction is warranted, it must correct the information as soon as reasonably possible. The organization must also, where reasonable, send a notification containing the correction to any organization it disclosed the information to (section 25(2)). Should an organization determine that no correction is necessary, it must make an annotation on the information that a correction was requested but not made (section 25(3)).

An organization cannot correct an opinion (section 25(5)). If an individual believes an opinion given in a reference is incorrect or contains an omission, the organization cannot correct or otherwise alter the opinion. But, the organization must make an annotation that a correction was requested. Errors in facts contained in a reference (e.g. the individual's record of absence) can be corrected when there is evidence of the inaccuracy.

An individual can make a complaint to the Information and Privacy Commissioner if he or she believes an organization has not made a reasonable effort to ensure the information collected or disclosed in a reference is accurate or complete, or if he or she disagrees with the decision of an organization not to correct the information (section 46(1)).

### **Examples of Consent Forms**

These forms are offered as examples only and do not constitute legal advice.

#### **A. Consent for organization to disclose employment reference information**

I, John Doe, hereby consent to ABC Corporation disclosing reference information relating to my employment with ABC Corporation when requested by an organization seeking to assess my suitability for a position with that organization.

This consent is valid for a period not exceeding one year from the date of signing.

\_\_\_\_\_  
(Signature of Candidate)

\_\_\_\_\_  
(Date)

#### **B. Consent for organization to obtain employment reference information**

Competition No. 123456

I, Jane Doe, hereby consent for the selection panel for this competition to contact

my past employer(s)

my present employer(s)

for the purpose of collecting reference information in order to assess my suitability for this position.

This consent is valid for a period not exceeding one year from the date of signing.

\_\_\_\_\_  
(Signature of Candidate)

\_\_\_\_\_  
(Date)

## **COLLECTION**

### **29. Can a store require a customer to provide a telephone number when making a purchase?**

An organization can only collect personal information, including a telephone number, for purposes that are reasonable, and to the extent reasonable for that purpose (section 11). The store could collect a customer's phone number with the customer's consent, as long as the purpose was reasonable and the phone number was required for that purpose. For example, this may be the case if the customer has asked to be contacted when a new product is received by the store.

An organization cannot require an individual to provide their phone number as a condition of the sale, if the phone number is not necessary to complete the sale. This would be the case for many retail transactions (section 7(2)).

## **SERVICE PROVIDERS**

### **30. Does PIPA permit an organization to use service providers outside of Canada to process or store client, customer or employee personal information?**

The Act does not prohibit organizations from using any service providers. However, if an organization's use of a foreign service provider means that personal information is collected, used or stored outside Canada the organization must include in its PIPA policies and practices the

names of the countries in which the activities are occurring or may occur, and the purposes for which the service provider has been engaged.

The organization must also provide notice to individuals about how they may obtain access to written information about the organization's policies and practices with respect to service providers outside Canada, and the name or position of a person who can answer questions about the use of the service provider.

## PROFESSIONAL REGULATORY ORGANIZATIONS

### 31. How does the Act affect professional regulatory organizations?

The Act establishes special provisions for professional regulatory organizations, such as the Law Society or APEGGA, to enable them to balance protection of personal information with their mandate to protect the public interest. Some of these organizations have been developing their own privacy codes. The Act allows professional regulatory organizations to develop and follow "personal information codes" that provide the same level of privacy protection as the Act. The Commissioner can hear privacy complaints made against professional regulatory organizations. Part 7 of the regulation elaborates on the provisions set out in section 55 of the Act. For more information on privacy information codes, see *Guidelines for Developing a Personal Information Code for Professional Regulatory Organizations*.

## NON-PROFIT ORGANIZATIONS

### 32. Does PIPA apply to non-profit organizations?

Some non-profit organizations are subject to the Act (section 56). Non-profit organizations are subject to the Act when they collect personal information as part of a commercial activity. For example, the Act applies when a non-profit organization registers individuals in a course or provides services for a fee, such as counseling or babysitting services. Another example would include the sale of goods that involves the collection of personal information, such as by mail order.

A non-profit organization includes an organization registered under the *Societies Act* or the *Agricultural Societies Act*, or Part 9 of the *Companies Act*. Non-profit organizations that do not carry out commercial activities are not subject to the Act. Personal employee information held by a non-profit organization is not subject to the Act. For more details, see *Frequently Asked Questions for Non-Profit Organizations* and *Information Sheet 1: Non-Profit Organizations*.

### 33. What is a commercial activity?

A commercial activity includes any transaction or any regular course of conduct that is of a commercial character. It includes the selling, bartering or leasing of donor, membership or other fundraising lists. A commercial activity also includes the operation of a private school or early childhood service program under the *School Act* and a private college under the *Post-secondary Learning Act* (section 56(1)(a)).

## SECURITY BREACH

### 34. What is a security breach?

A security breach is a loss of or unauthorized access to or disclosure of personal information. Examples include when a laptop containing personal information is stolen, or personal information is mistakenly e-mailed to the wrong person.

### 35. What are an organization's responsibilities if a security breach occurs?

An organization must, without unreasonable delay, notify the Information and Privacy Commissioner if an incident occurs that involves loss of or unauthorized access to or disclosure of personal information that may pose a real risk of significant harm to individuals (section 34.1).

The Commissioner may then require the organization to notify affected individuals (section 37.1). Despite section 34.1, an organization may also, on its own initiative, notify individuals affected by a security breach (section 37.1(7)).

**36. What is a “real risk of significant harm”?**

A “real” risk is more than merely speculative. It is a genuine risk, not a risk that is merely theoretical or hypothetical. “Significant” harm is harm of importance or consequence. For example, the theft from a vehicle of a laptop computer containing an unencrypted database of personal information relating to financial transactions is likely to pose a real risk of significant harm to the individuals the information is about.

**ACCESS**

**37. What is the process when an individual wants to access his or her own personal information from an organization?**

An individual must make a request in writing to an organization and provide sufficient detail to enable the organization to identify the information (section 26). The individual may ask for a copy of the record or to examine the record. Organizations have 45 days to respond, and may extend the response period by 30 days in some circumstances (sections 28 and 31). An organization may charge a reasonable fee for providing access (section 32) but may not charge a fee for personal employee information (section 32(1.1)). If an organization refuses access to any part of the personal information, it must provide reasons for refusal and the provisions of the Act on which the refusal is based (section 29). Individuals may appeal an organization’s decisions to the Commissioner (section 46).

**COMPLAINTS**

**38. What can an individual do if he or she believes that their personal information has been collected in contravention of the Act?**

An individual can complain to Alberta’s Information and Privacy Commissioner (section 46). This is the same Commissioner who oversees the *Freedom of Information and Protection of Privacy Act* and the *Health Information Act*. The Commissioner has general oversight of the Act, including the power to conduct investigations, hold inquiries and issue binding orders (section 36). If the Commissioner determines that an organization has breached the Act, an individual can apply to court to recover damages for loss or injury he or she may have suffered as a result of the breach of the Act (section 60).

**39. Can an organization or individual be sued?**

An individual can make a complaint about a breach of privacy under the *Personal Information Protection Act*. There are three different processes of redress.

First, the individual can make a complaint to the Office of the Information and Privacy Commissioner against an organization (section 46). The Commissioner’s staff would investigate, mediate, and if a solution could not be reached in mediation, the Commissioner may hold an inquiry. The Commissioner would issue an Order, where he may find the organization at fault or not. This will be the normal channel for complaints.

Secondly, the Act provides for fines to be assessed by the courts. The fines only come into play when an organization or individual has been found guilty of an offense under the Act. The offenses are described in section 59. These cover actions that contravene the Act, such as hacking into a database to steal credit card numbers. Fines are assessed by the courts, not by the Information and Privacy Commissioner.

Similar fines are included in Alberta’s *Freedom of Information and Protection of Privacy Act* that covers the public sector. No fines have been levied since that Act came into effect in 1995.

Note that section 57 of the Act provides protection for organizations and employees who are acting in good faith under the Act. Committing an error in good faith under the Act is distinguished from committing an offence.

Thirdly, an individual can sue an organization for damages for loss or injury after the Commissioner has made an Order against an organization (section 60). The individual has to have suffered some loss to be able to receive compensation. An individual can sue for damages for loss or injury against a person (a business or individual) who has been convicted of an offence under the Act.

**40. Will the Act protect a whistleblower, i.e. an employee who discloses information regarding a possible breach of the Act by his or her employer?**

The Act prohibits an organization from taking any adverse employment action against an employee, when the employee has acted in good faith in providing information to the Commissioner (section 58).

**41. Where can I obtain more information?**

Additional information and resources about PIPA are available on the websites of Access and Privacy, Service Alberta, and the Office of the Information and Privacy Commissioner.

**Access and Privacy  
Service Alberta**

Phone: 780-644-PIPA (7472) Toll free dial 310-0000  
E-mail: [pspinfo@gov.ab.ca](mailto:pspinfo@gov.ab.ca)  
Website: [pipa.alberta.ca](http://pipa.alberta.ca)

**Office of the Information and Privacy Commissioner**

Phone: 403-297-2728 Toll free dial 1-888-878-4044  
E-mail: [generalinfo@oipc.ab.ca](mailto:generalinfo@oipc.ab.ca)  
Website: [www.oipc.ab.ca](http://www.oipc.ab.ca)