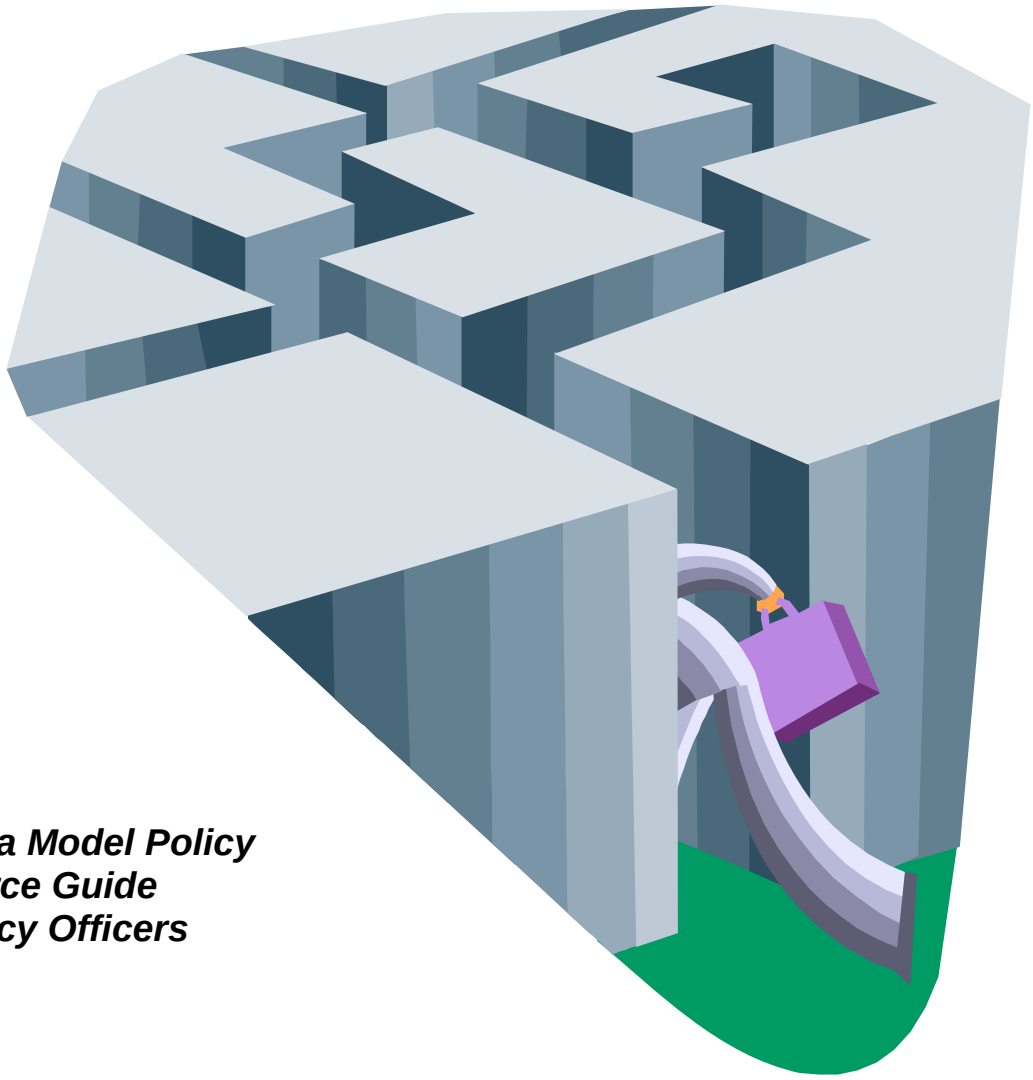
Privacy Legislation & Your Organization

A Tool Kit for the Alberta Construction Industry



Includes a Model Policy
& Resource Guide
For Privacy Officers

An Alberta Construction Industry Initiative Developed in Collaboration with:

Alberta Construction Association
Alberta Home Builders' Association
Alberta Roadbuilders & Heavy Construction Association
Construction Labour Relations – An Alberta Association
Merit Contractors Association
Progressive Contractors Association of Canada

Released December 2003 Revised May 2008

Table of Contents

Please Note: All terms formatted in ***bold and italics*** may be found in the *Definitions* section.

What You Need To Know…
About Alberta's *Personal Information Protection Act*

This summary document is intended to assist Alberta's construction industry deal with privacy legislation that becomes effective January 1, 2004.

Bill 44, the *Personal Information Protection Act (PIPA)*, was passed during the Fall Session of the Alberta Legislature and governs the collection, use, disclosure and access to **personal information** held by all provincially regulated organizations doing business in Alberta.

It's important to understand that this new Act affects the way companies manage information they obtain from customers and potential customers, and also how they handle information from their employees.

Alberta's legislation coincides with the federal government's *Personal Information and Electronic Documents Act (PIPEDA).* Part 1 of that Act also goes into effect on January 1, 2004, and deals with information held by federally regulated organizations or those operating outside Alberta. If your firm conducts business outside Alberta, then it is your responsibility to find out about privacy laws in other provinces. It may be best to seek a legal opinion regarding your operations outside Alberta.

What You Need To Do

1. Put someone in charge
2. Become familiar with the Act
3. Review how your organization handles, stores, and passes on personal information
4. Determine if your organization's information handling process measures up to the Act
5. Develop privacy policies and practices. The *Model Policy* created for the Alberta construction industry can help a great deal in handling this for you.
6. Train staff to ensure they are familiar with what's required
7. Develop "access to information" and "complaints-handling" processes
8. Review and revise forms to make sure they comply with the Act
9. Review and revise contracts to ensure that the information you pass on to others is adequately protected
10. Consider employees' personal information.

How You Have To Operate

Generally, it is now against the law to obtain personal information about anyone and use that information for a reason that the person did not agree to. For example, if a company got a person's name, home address, and personal phone number at a Trade Show through a contest entry form, and then used that information to contact that person regarding a potential sales opportunity, the company could be violating the Act.

In the same fashion, companies may need to get consent from people to use that information for marketing reasons. If a person provides personal information for the company on any form or document, it's the company's responsibility to inform that person that the information may be used for purposes other than what may be evident. A company may then contact that person if consent is given on the form.

Your organization is responsible for all personal information in your custody or under your control. In other words, even information that you send to another party such as a contractor. For example, if a company asks for payroll records on a "cost-plus" job, your company must be very careful to ensure that only specific information is released. This may mean that your computer systems and information handling processes need to be changed. An example would be information passed along to another organization. This should contain no personal information, unless the person agreed to have that information circulated to other parties.

Penalties

If you knowingly contrive *PIPA*, you may face penalties of up to $10,000 for an individual and up to $100,000 for the organization.

Consent Must Be Obtained

Generally, organizations need to obtain individual consent before collecting, using and disclosing personal information, except in ~~the~~ certain cases involving~~case of~~ employee information.

Consent may be:

- Express: either written or oral
- Implied
- Opt-out. This means a company may state on a form that unless the person objects, the company will use the information for reasonable purposes.

In determining what type of consent is appropriate, consider what is reasonable for the person, the circumstances, and the sensitivity of the information. Also remember that at some time you may need to prove that you gained consent, so it would be best to get the consent in writing, but if that's not the case, make sure you document when and where the person gave you consent orally. For example, if a customer (a person, not a corporation) gave a company the right to use them as a reference, the company should have that consent documented. Ensure you only pass along specific information about the person providing the reference, such as name and phone number or e-mail address.

There Are Exceptions

In some situations you do not need to obtain consent, including the following examples:

- When the collection of information is clearly in the individual's interests and consent cannot be obtained in a timely manner, or the individual wouldn't reasonably be expected to withhold consent.
- Personal information collected before January 1, 2004, is deemed to have been collected with consent but only for the original, limited purpose for collecting it
- In some circumstances, ~~Y~~you may collect, use and disclose personal employee information without consent if the individual is an employee, or if you are recruiting an employee.

A Person Can Withdraw or Change Consent

- In most situations, individuals can change or withdraw consent but not if it interferes with a legal obligation.

Personal Employee Records

- You may collect, use and disclose personal employee information without consent if the individual is an employee, or if you are recruiting an employee.
- The collection, use and disclosure of personal information must be reasonable for the purpose and limited to establishing, managing or terminating the work or volunteer relationship.
- You must notify the employee, before collecting the information, that the information is going to be collected and of the purposes for which it is going to be collected.
- You have to store personal employee information in a secure manner, so other employees or people from outside the organization can't readily have access to it.

What If Somebody Asks To See Their Info?

Individuals have the right to:

- Ask for access to their own personal information
- Know how their information is, or has been used
- Know to whom and under what situations the information is or has been disclosed
- In some cases, the Act authorizes another person to act on behalf of the individual when exercising their rights, for example, a parent on behalf of a child

You Can Refuse Access to Personal Info

- In some circumstances, organizations can or must refuse access such as when disclosure would harm someone, an investigation, or legal proceeding

Fees

- Organizations may charge a reasonable fee to cover their out-of-pocket costs for retrieving information upon the request of individuals. Companies must respond to these requests within 45 calendar days.

Right to Appeal

- Individuals may ask Alberta's Information and Privacy Commissioner to review an organization's decision if there's a disagreement.

The Information Must Be Accurate and Secure

Organizations must:

- Take reasonable steps to ensure information is accurate, up-to-date, complete, and not misleading
- Use reasonable safeguards to protect personal information from theft, modification, unauthorized access, collection, use, disclosure and destruction

If the Information Is Wrong

- Individuals may ask organizations to correct their information if the organization's records contain errors or omissions
- Organizations must correct any error or omission and, if reasonable, inform other organizations to which the incorrect information was disclosed of the change

What You Need To Do…

This list is not a comprehensive list of what is required for organizations/companies to comply with provincial privacy legislation, but does offer a place to start.

A. Audit your organization's personal information practices

1. What personal information do we collect?
2. What personal information do we need to operate (establishing, managing, or terminating employment relationship, provide the service or product we offer)?
3. Is it necessary to collect all the personal information that we do?
4. If not, why do we collect the extra personal information (i.e. what do we do with it?)
5. Do we want to continue collecting the extra personal information?
6. If so, should we give the customer the option of opting out of providing this extra personal information?
7. Do we disclose personal information to any third parties?
8. To whom do we disclose it?
9. Is it necessary to disclose it?
10. If not necessary do we want to continue disclosing it?
11. If so, should we give the customer the option of opting out of having the personal information disclosed?
12. By what means do we collect it (written forms, telephone conversations, e-mail)?
13. Do we collect personal employee information? Do we use and disclose that information? Do we provide our employees with reasonable notice of the purposes for which the information is going to be collected?
14. Where and how do we store personal information?
15. Who has access to it?
16. Do we need additional safeguards?
17. How long do we retain personal information?
18. Do we ever destroy it?
19. Can we destroy it? Should we destroy it? Do we need to keep it?
20. How would we gather personal information if a customer made an access request?

B. Appoint a Privacy Officer

1. designate one or more staff
2. confirm senior management has delegated authority for privacy to these individuals
3. inform all staff who the designated privacy officers are

C. Develop a privacy policy

1. You may find the Model Policy in this document sufficient to adopt for your organization or to use as a reference to develop your own policy statement. Review of your policy by legal counsel is recommended

D. Develop procedures and appropriate documentation to deal with:

1. obtaining or confirming consent (for existing uses of existing information, for new uses for existing information, for new information)
2. notifying employees of the purposes for which their personal employee information is going to be collected
3. questions and concerns from employees and/or customers
4. access to information by staff
5. access requests from employees and/or customers
6. disclosure to third parties
7. correction requests
8. withdrawals or variations of consent; and
9. retention and destruction of personal information

E. Revise existing records (Payroll files, employee and customer information databases) and documents (Application forms, employee forms, websites, brochures, etc.)

F. Review contracts with third party service providers to ensure compliance with legislation

G. Ensure appropriate safeguards are in place to protect personal information

H. It is strongly recommended that you develop a process to handle complaints

I. Inform, educate, and train your staff (Human resources, payroll, safety, customer service, marketing, supervisory)

J. Communicate your policy to third parties (customers, suppliers)

K. Do a periodic review of your policy and procedures to ensure compliance

REVISED Model Policy

Introduction

The protection of personal information is important to [*insert organization's name*] and we have a policy and procedures dealing with the protection of privacy. Any questions about this policy can be directed to our Privacy Officer, [*you may insert Privacy's Officer's name*] at [*insert contact number etc. for Privacy Officer*].

Our employees play an important role in protecting personal information. Our employees are required to adhere to this policy and take all reasonable steps to ensure that personal information is protected from unauthorized access.

Collection, Use and Disclosure of Personal Information

[*Include this paragraph if you are a contractor and do not normally deal with individuals as customers. Delete the following two paragraphs*] Our organization does not usually collect personal information from individuals as customers (other than business contact information), since we generally deal only with other companies. In the event that we do collect personal information from an individual customer, that information will only be used by us to administer the contract for the product and/or services. When we do deal with individuals as customers we collect the following types of personal information:

[*Include this paragraph if you have a retail business and regularly collect personal information from customers. Delete the preceding paragraph and the following paragraph.*] We collect personal information from our customers in order to administer the contract for products and/or services. We collect the following types of personal information from our customers:

[*Include this paragraph if you are both a contractor and a retailer and regularly collect personal information from customers – delete the preceding two paragraphs*] Although we deal commonly with other companies and in those cases do not collect personal information other than business contact information, we also deal with individual customers. We collect the personal information of our individual customers in order to administer the contract for products and/or services. When dealing with these individual customers we collect the following types of personal information:

1. Customer name;
2. Customer address and telephone number;
3. [*Include in this list other examples of the types of personal information you collect – the list does not have to be exhaustive but should provide good examples of the type of information you collect*]

This personal information is collected for the following purposes:

[*This list should describe the reasons that you collect personal information – what do you use the information for? For example:*

1. *In order to contact the customer for instruction and billing purposes;*
2. *For the administration of the contract for services;*]

We only collect personal information directly from the customer except when we have the customer's consent to collect information from elsewhere or are permitted by law to collect it without the customer's consent.

We only use a customer's personal information for the purposes outlined above. If we need to use the personal information for any other purpose we will contact the customer and obtain consent prior to that use.

We disclose customers' personal information to the following third parties:

1. [*This list should include the names of all third parties to whom you disclose personal information, if any.*]

We disclose this information in order to [*insert reason for disclosing the personal information*.] We do not disclose personal information to third parties for any other purposes.

Our customers have the right to withdraw consent for our collection, use or disclosure of their personal information at any time. However, if a customer does so it may affect his/ her ability to [*insert whatever the applicable product or service is*.] If a customer wishes to withdraw consent, or has any questions about withdrawing consent, he or she can contact our Privacy Officer.

Business contact information is not protected by this policy. This type of information is not considered to be personal information and may be collected, used and disclosed without consent.

Consent

In most cases customers consent to us collecting, using and disclosing personal information for the purposes outlined above by simply agreeing to provide us with the personal information. [*If you collect, use or disclose personal information for any purposes other than simply providing the product or service – for example, for your mailing list or for disclosure to others in your industry for their mailing lists - include the following sentences.*] However, there may be cases where we require explicit consent, including [*insert the other uses and disclosures*]. The withdrawal of this consent will generally not affect a customer's ability to obtain the product or service they require, however by providing us with consent for the previously outlined uses we can [*insert examples of why the customer might want to allow you to use their information for other uses or disclosures, for example -.serve the customer better / offer the customer alternatives, etc.*]

Storing your Personal Information

We only keep personal information for as long as is necessary for the purposes outlined above. This may include keeping the information after a project is completed in order to resolve any problems or concerns that may arise. We are also required by law to maintain certain records for set amounts of time. We have appropriate safeguards in place to protect personal information and when we no longer need the information it is destroyed. We try to keep personal information as accurate as possible and customers can assist us by providing us with updated information when necessary. Information can be updated by contacting [*insert name of Privacy Officer*].

Access

Our customers have the right to access the personal information we hold about them. A customer can access his/her personal information by making a request to our Privacy Officer. The Officer will provide the necessary forms and assistance to make the request and obtain the information. If the customer believes that some of the personal information is incorrect he or she can request that the information be corrected.

We may charge our customers for out-of-pocket expenses in responding to an access request. If we decide that a charge is appropriate we will provide the customer with a written estimate prior to providing access. Any concerns with the estimated charge should be directed to our Privacy Officer.

Accountability

We apply our best efforts to protect our customer's privacy. If our customers have any concerns they are free to contact our Privacy Officer. We hope that the Officer will be able to resolve any problems. If concerns are not resolved, the Officer can provide information on making a formal complaint.

Collection, Use and Disclosure of Personal Employee Information

[*The following information is only for your employees – you may wish to provide this information to your employees as a separate document or you may wish to have two versions of your policy – one for external audiences and one for internal audiences.*]

"Personal employee information" is personal information collected, used or disclosed for the purposes of establishing, managing or terminating an employment relationship. We can collect, use and disclose this information without consent but we will only collect, use and disclose the personal information that is necessary for the purpose of administering the employment relationship. "Personal employee information" may include the following:

1. name;
2. home address and phone number;
3. employment history;
4. disciplinary record;
5. alcohol and drug testing results;
6. medical information or disability;
7. social insurance number;
8. age;
9. bank account;
10. wage or salary paid;
11. sex;
12. family status;
13. marital status.

We may collect and use this information as reasonably required for the purposes of establishing, managing or terminating the employment relationship between the organization and the individual. The information may be disclosed to various decision-makers within the organization, and/or to third parties, for the same purposes. Specific purposes may include, but are not limited to:

- providing benefits (including referrals for EFAP benefits),
- paying wages,
- managing and responding to workplace investigations, including safety investigations

- managing WCB claims;
- developing return to work agreements and modified work programs;
- overseeing implementation and enforcement of workplace policies, including safety policies;
- managing and addressing civil claims and insurance matters.

Third parties to whom personal employee information may be disclosed for the purposes outlined above include:

1. *benefit provider (including provider of EFAP benefits);*
2. *payroll company;*
3. *union;*
4. *WCB; and*
5. *insurance companies.*

Our personal employee information is safeguarded to prevent unauthorized access, use and disclosure. Particularly sensitive information such as medical information is stored separately and is only accessed by those with a need to do so.

It is important that we keep our personal employee information as up to date as possible. Please notify us as soon as possible of any changes to employee contact information or beneficiary / dependent information.

Employees may access their personal employee information by making a request to [*insert name of Privacy Officer*.] Any concerns about the collection, use or disclosure of personal employee information can also be addressed by this individual. Please feel free to contact [*insert name of Privacy Officer*] with any questions.

Resource Guide For Privacy Officers

It is strongly suggested that your organization's Privacy Officer becomes familiar with the actual *PIPA* legislation. More information about *PIPA* is provided on the *PIPA* web site at http://www.psp.gov.ab.ca. If you have a question about PIPA, you can call the PIPA Help Desk at (780)-644-PIPA (7472), (toll free dial 310-0000 first and then the number within Alberta).

Introduction and Background

The following section is intended for the use of employees working as Privacy Officers for their organization.

Please note this section is not meant to be a legal document and is not legally binding. It's simply a guideline document designed to assist your Organization's Privacy Officer. All the words printed in ***bold and italics*** are in the Definitions section at the back of this document.

Standard of Review

The actions of any organization in complying with the legislation will be measured on a standard of reasonableness – "what would a reasonable person consider reasonable under the circumstances?"

Geographical Scope

The *Personal Information Protection Act (PIPA)* applies to all Alberta ***organizations*** unless they are federally regulated or involved in certain cross-border personal information transfers. If you have any doubt about whether *PIPA* applies to your ***organization*** or the personal information you hold, you should obtain legal advice.

Purpose

The purpose of *PIPA* is to set rules for the ***collection, use,*** and ***disclosure*** of ***personal information*** that balances both:

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

There are certain exceptions to which PIPA does not apply. Please see *Schedule1 – Personal Information to which PIPA does not apply*). *PIPA* applies to all personal information collected by an ***organization***.

Personal Information Collected prior to 2004

Personal information collected prior to January 1, 2004:

1. is deemed to have been ***collected*** pursuant to ***consent*** given by that individual,
2. may be ***used*** and ***disclosed*** by the ***organization*** for the purposes for which it was ***collected****,* and
3. is to be treated in the same manner as ***personal information collected*** under *PIPA*.

Contracting Out of the Legislation

An ***organization*** cannot make an agreement with an individual to waive that individual's rights under *PIPA*. Such an agreement will be found to be void and not binding.

Applicable Legislation

PIPA sets out the minimum requirements for the protection of personal information. Having said this, you must take into account other legislation or obligations that require your ***organization*** to collect, use, disclose or retain personal information (for example – Income Tax Act, Workers Compensation Board information, and defending a possible lawsuit etc.)

The Ten Principles of the *Personal Information Protection Act* in Summary

1. Accountability

The ***organization*** is responsible for ***personal information*** under its control and shall designate an individual or individuals who are accountable for the ***organization's*** compliance with the following principles.

2. Identifying Purposes

The purposes for which ***personal information*** is ***collected*** shall be identified by the organization at or before the time the information is ***collected.***

3. Consent

The knowledge and ***consent*** of the individual are required for the ***collection, use*****,** or ***disclosure*** of ***personal information***, except where inappropriate.

4. Limiting Collection

The ***collection*** of ***personal information*** shall be limited to that which is necessary for the purposes identified by the organization. Information shall be ***collected*** by fair and lawful means.

5. Limiting Use, Disclosure, and Retention

Personal information shall not be ***used*** or disclosed for purposes other than those for which it was collected, except with the ***consent*** of the individual or as required by law. ***Personal information*** shall be retained only as long as necessary for the fulfilment of those purposes.

6. Accuracy

Personal information shall be as accurate, complete, and up-to-date as necessary for the purposes for which it is to be ***used***.

7. Safeguards

Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

8. Openness

The ***organization*** shall make readily available to individuals specific information about its policies and practices relating to the management of ***personal information*****.**

9. Individual Access

Upon request, an individual shall be informed of the existence, ***use***, and ***disclosure*** of his or her ***personal information*** and shall be given access to that information. An individual shall

be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

10. Challenging Compliance

An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the ***organization's*** compliance.

Accountability and Administration

1) You must develop and implement policies and procedures dealing with the protection of ***personal information***. The policy must be made available to the public upon request. The policy should include:
    a. A description of the types of ***personal information*** held by the ***organization***;
    b. The reason personal information is collected by the organization;
    c. How personal information is used by the organization;
    d. To whom personal information is disclosed by the organization;
    e. The name of the organization's privacy officer
    f. The name of the person to whom complaints should be directed;
    g. The form such complaints should take;
    h. How to make a personal information access request

2) You must appoint a privacy officer who will have the responsibility of ensuring the ***organization's*** compliance with the legislation.

3) The privacy officer must be vested with the authority necessary to carry out his or her responsibilities under the legislation.

4) You must develop procedures and time frames for complying with requests for access to *personal information* held by the organization. Please see *Schedule 2 – Dealing with an Access Request.*

5) You must ensure that staff is adequately trained to ensure that the policies and procedures can be effectively implemented.

6) If your ***organization*** engages the services of a contractor, you are responsible for the compliance of that contractor with *PIPA* with respect to the services offered by that contractor.

Consent

1) Generally, in order to collect, ***use*** or ***disclose personal information*** about an individual your ***organization*** must have ***consent*** to do so.

2) Your ***organization*** cannot, as a condition of supplying a product or service, require an individual to ***consent*** to the ***collection, use*** or ***disclosure*** of ***personal information*** unless that collection, use or disclosure is necessary to provide the product or service.

3) An individual may give his or her ***consent*** in writing or orally.

4) An individual is deemed to ***consent*** to the ***collection, use*** or ***disclosure*** of ***personal information*** by your ***organization*** for a particular purpose if:

    (a) the individual, without actually specifically giving ***consent*** voluntarily provides the ***personal information*** to your ***organization*** for the purpose that has been described to the individual, and

    (b) it is ***reasonable*** **t**hat a person would voluntarily provide that ***personal information*** in the circumstances.

5) Notwithstanding the requirement for consent, your ***organization*** may ***collect, use*** or ***disclose personal information*** about an individual for particular purposes if

(a) your ***organization*** provides the individual with a notice that it intends to ***collect, use*** **or** ***disclose personal information*** about the individual for those purposes, and gives the individual a reasonable opportunity to decline or object to having his or her ***personal information collected, used*** or ***disclosed*** for those purposes,

(b) the individual does not, within a ***reasonable*** time, give to the ***organization*** a response to that notice declining or objecting to the proposed ***collection, use*** or ***disclosure***, and

(c) you have regard for the level of the sensitivity, if any, of the ***personal information*** in the circumstances, it is ***reasonable*** to ***collect, use*** or ***disclose*** the ***personal information***.

6) ***Consent*** in writing may be given by electronic means if the ***organization*** receiving the electronic consent produces, or is able at any time to produce, a copy of the ***consent*** in paper form.

7) An individual may withdraw or vary his or her ***consent*** to the ***collection, use*** or ***disclosure*** of his or her ***personal information*** by your ***organization***

8) If you are advised by an individual that he or she wishes to withdraw or vary the ***consent***, you must inform the individual of the likely consequences of withdrawing or varying the ***consent***.

9) You are not required to inform the individual of the consequences if the likely consequences of withdrawing or varying the ***consent*** would be ***reasonably*** obvious to the individual.

10) Except where the ***collection, use*** or ***disclosure*** of ***personal information*** without ***consent*** is permitted under *PIPA*, if an individual withdraws or varies ***consent*** to the ***collection, use*** or ***disclosure*** of ***personal information*** you must

(a) in the case of the withdrawal of the ***consent***, stop ***collecting, using*** or ***disclosing*** the ***personal information***, or

(b) in the case of a variation of the ***consent***, abide by the ***consent*** as varied.

11) If withdrawing or varying ***consent*** would frustrate the performance of a legal obligation, then any withdrawal or variation of the ***consent*** would not be permitted to the extent that the withdrawal or variation would frustrate the performance of the legal obligation owed between those parties.

12) If ***consent*** was given orally the individual can withdraw or vary the consent by making an oral request.

13) You must not obtain or attempt to obtain ***consent*** to the ***collection, use*** or ***disclosure*** of ***personal information*** by providing false or misleading information, or by using deceptive or misleading practices.

Limitations on Collection

1) Your ***organization*** may ***collect personal information*** only for purposes that are ***reasonable*** and generally, only with the ***consent*** of the individual.

2) When your ***organization collects personal information***, it may do so only to the extent that is ***reasonable*** for meeting the purposes for which the information is collected.

3) You can ***collect personal information*** about an individual without ***consent*** in certain circumstances. These circumstances are set out in ***Schedule 3—Collection, Use and Disclosure without Consent*.**

4) Before or at the time of ***collecting personal information*** from the individual, you must notify that individual in writing or orally as to the purposes for which the information is collected and the name of your privacy officer.

5) Notification may also be required when ***personal information*** is ***collected*** from another ***organization***. For information regarding notices required when collecting information from other ***organizations***. Please see *Schedule 4—Notices Required when sharing Personal Information with other Organizations*.

Limitations on Use

1) Your ***organization*** can ***use personal information*** only for purposes that are ***reasonable*** and generally, only with the ***consent*** of the individual.

2) When your ***organization uses personal information***, it can do so only to the extent that is ***reasonable*** for meeting the purposes for which the information is ***used***.

3) In certain circumstances ***personal information*** can be used without ***consent***. Please see *Schedule 3—Collection, Use and Disclosure without Consent*.

Limitations on Disclosure

1) Your ***organization*** can ***disclose personal information*** only for purposes that are ***reasonable*** and generally, only with the ***consent*** of the individual.

2) When your ***organization discloses personal information***, it may do so only to the extent that is ***reasonable*** for meeting the purposes for which the information is ***disclosed***.

3) There are exceptions to the requirement for ***consent*** for ***disclosure***. Please see *Schedule 3—Collection, Use and Disclosure without Consent*.**

Personal Employee Information

1) Your ***organization*** may ***collect, use*** *or* ***disclose personal employee information*** about an individual for the purposes of establishing, managing or terminating an employment (or volunteer) relationship without the ***consent*** of the individual if

    1) the individual is an employee (or volunteer) of the ***organization***, or,

    2) the ***collection*** of the information is for the purpose of recruiting a potential employee.

    3) Your ***organization*** shall not ***collect, use*** *or* ***disclose personal employee information*** about an individual unless the ***collection, use or disclosure*** is ***reasonable*** for the purposes of establishing, managing or terminating the employment relationship.

    4) You must provide employees with notice as to the purposes for ***collecting***, ***using*** and ***disclosing*** their personal employee information prior to doing so. This can be achieved by appropriately drafting recruitment information and policy manuals and by providing notification when circumstances change (for example, a change in benefit provider).

    5) If you are ***collecting***, ***using*** or ***disclosing personal employee information*** for the purposes of an employment related investigation you are not required to provide prior notice. There may be other circumstances where you are not required to provide prior notice. Please see *Schedule 3—Collection, Use and Disclosure without Consent.*

    6) Your ***organization*** can ***disclose personal information*** about a former employee without ***consent*** for the purposes of a reference check.

Access

1) Upon written request, your ***organization*** must provide an individual with access to, and information concerning the existence, ***use*** and ***disclosure*** of his or her ***personal information***. You must provide information about the purpose for which the personal information has been, and is being, used and the names of any persons to whom the personal information has been, or is being, disclosed. You can refuse access to certain personal information. Please see *Schedule 5 – Refusing Access*

2) If you can sever the information that may not, or must not be released, you must sever that information and provide access to the rest of the ***personal information***.

3) The individual who is asking for access can ask for a copy, or ask to actually see the record that contains the ***personal information***.

4) If ***personal information*** is stored electronically you must provide a hard copy of the record if the record can be created using your ***organization's*** normal computer hardware and expertise and, creating the record would not unreasonably interfere with the operations of your ***organization***.

5) You must respond to the access request within the time limits set out in the legislation. These time limits should be taken into account in the process that your ***organization*** has developed for dealing with access requests. Please see *Schedule 2 – Dealing with an Access Request.*

6) Your ***organization*** can charge a fee to process an access request; however, the fee can only cover out-of-pocket expenses such as photocopying costs.

7) If you intend to charge a fee, you must give the applicant a written estimate of the fee before providing the service. You can require the applicant to pay a deposit in an amount determined by your ***organization***. The time limits are interrupted until the estimate is accepted and deposit paid if required. If the applicant does not respond to the estimate within 30 days you may consider the request to have been withdrawn. If you charge a fee you can refuse to release their ***personal information*** until the fee is paid in full.

8) If you receive an access request you must assist the applicant and respond as accurately and completely as possible. You cannot charge a fee for access request made by an employee.

Right of Correction

1) An individual has the right to ask that information relating to him or her be corrected. The correction must be made as soon as possible.

2) If there is disagreement about whether certain information should be corrected, and you decide not to correct the information, you must note the individual's disagreement with the ***personal information*** and keep that note with the personal information in question.

3) If a correction is made you must notify any ***organizations*** to which the incorrect information was disclosed of the correction.

4) If you receive a notification of the type referred to in the prior paragraph you must make any relevant corrections.

5) You must not correct or otherwise alter an opinion.

Accuracy

1) ***Personal information*** must be as accurate, complete, and as up-to-date as practicably possible for the purpose for which the information was collected.

Security

1) Your ***organization*** must develop ***reasonable*** security measures to limit unauthorized access, ***use*** and ***disclosure*** of ***personal information*** in the custody or control of the ***organization***.

Retention

1) ***Personal information*** must be retained for only as long as is reasonably necessary to fulfill the purpose for which it was ***collected***. Remember that the length of time that personal information must be retained may be governed by other legal requirements or business purposes. Examples could include tax laws, asbestos-related issues, Workers Compensation Board, or business purposes.

Disposal

1) Your ***organization*** must develop guidelines and procedures to govern the secure destruction of ***personal information*** once it is no longer required

Complaints

1) As individuals may wish to file a complaint with your *organization* concerning compliance with the legislation, you should develop a process for addressing complaints. Having an internal complaint process may help to prevent an individual from filing a complaint with the Provincial Privacy Commissioner.

2) Your internal complaint process may require that all complaints be in writing.

3) Upon review, if a complaint is justified, your ***organization*** should take appropriate measures to rectify the problem in a timely manner.

4) Your ***organization*** must inform an individual filing a complaint that he or she may ask for a review under section 46 of the *Personal Information Protection Act*.

Schedule 1 – Personal Information to Which PIPA Does Not Apply

Reference: *Section 4 – Personal Information Protection Act*

(a) The collection, use or disclosure of personal information if the collection, use or disclosure, as the case may be, is for personal or domestic purposes of the individual and for no other purpose;

(b) The collection, use or disclosure of personal information if the collection, use or disclosure, as the case may be, is for artistic or literary purposes and for no other purpose;

(c) the collection, use or disclosure of personal information, other than personal employee information that is collected, used or disclosed pursuant to section 15, 18 or 21, if the collection, use or disclosure, as the case may be, is for journalistic purposes and for no other purpose;

(d) the collection, use or disclosure of business contact information if the collection, use or disclosure, as the case may be, is for the purposes of contacting an individual in that individual's capacity as an employee or an official of an organization and for no other purpose;

(e) Personal information that is in the custody of an organization if the *Freedom of Information and Protection of Privacy Act* applies to that information;

(f) health information as defined in the *Health Information Act* where that information is collected, used or disclosed by an organization for health care purposes including health research and management of the health care system, but for the purposes of this clause health information does not include personal employee information;

(g) The collection, use or disclosure of personal information by an officer of the Legislature if the collection, use or disclosure, as the case may be, relates to the exercise of that officer's functions under an enactment;

(h) Personal information about an individual if the individual has been dead for at least 20 years;

(i) Personal information about an individual that is contained in a record that has been in existence for at least 100 years;

(j) Personal information contained in any record transferred to an archival institution where access to the record was unrestricted or governed by an agreement between the archival institution and the donor of the record before the coming into force of this Act;

(k) personal information contained in a court file, a record of a judge of the Court of Appeal of Alberta, the Court of Queen's Bench of Alberta or The Provincial Court of Alberta, a record of a master in chambers of the Court of Queen's Bench of Alberta, a record of a sitting justice of the peace or a presiding justice of the peace under the *Justice of the Peace Act*, a judicial administration record or a record relating to support services provided to the judges of any of the courts referred to in this clause;

(l) Personal information contained in a record of any type that has been created by or for:

i) A Member of the Legislative Assembly, or

(ii) An elected or appointed member of a public body;

(m) The collection, use or disclosure of personal information by a registered constituency association or a registered party as defined in the *Election Finances and Contributions Disclosure Act*;

(n) the collection, use or disclosure of personal information by an individual who is a bona fide candidate for public office where the information is being collected, used or disclosed, as the case may be, for the purposes of campaigning for that office and for no other purpose;

(o) Personal information contained in a personal note, communication or draft decision created by or for a person who is acting in a judicial, quasi-judicial or adjudicative capacity.

Schedule 2 – Dealing With An Access Request

Reference: *Sections 24, 26, 27, 28, 29, 30, 31 Personal Information Protection* Act

1. On the request of an individual for access your organization must provide the individual with access to the following:
    1. The individual's personal information where that information is contained in a record in the custody of or under the control of the organization
    2. The purposes for which that personal information has been used and is being used
    3. The names of the people to whom, and the circumstances in which, the personal information has been, and is being, disclosed

2. Your organization must respond to the applicant's request not later than 45 days from the day on which you received the written access request unless you get an extension on that time period from the Privacy Commissioner. There are two circumstances which extend the 45 day period by virtue of operation of the statute – please see section 28 of the legislation.

3. Your response to the access request must include the following:
    1. Advice as to whether or not the individual is entitled to or will be given access to all or part of his or her personal information
    2. Advice as to when access will be given (if the individual wants to see the original records rather than just copies or if it is not reasonable to reproduce a certain record)
    3. If applicable, advice as to why access has been refused to certain personal information
    4. If applicable, advice at to whom can answer any question regarding the refusal
    5. Advice as to the fact that the individual can ask for a review of refusal by the Privacy Commissioner under section 46 of PIPA
    6. If applicable, copies of the actual records or if there is a delay in providing copies of the records, the reason for the delay
4. You may extend the time period for responding to a request by 30 days, or longer with the Commissioner's permission if:
    1. The applicant does not give enough detail to enable the organization to identify the personal information or the record relating to the information; or
    2 a large amount of personal information is requested or must be searched; or
    3. Meeting the time limit would unreasonably interfere with the operations of the organization; or
    4. more time is need to consult with another organization or with a public body before the organization is able to determine whether or not to give the applicant access to the requested personal information or record relating to the information.

5. If you do extend the time limit you must inform the applicant of:
    1. The reason for the extension;
    2. The time when a response can be expected; and
    3. The fact that the applicant can ask for a review of the extension under s.46 of PIPA

Schedule 3 – Collection, Use and Disclosure Without Consent

Reference: *Sections 14, 17 and 20 Personal Information Protection Act*

Your organization may collect personal information about an individual without the consent of that individual if

(a) a reasonable person would consider that the collection of the information is clearly in the interests of the individual and consent of the individual cannot be obtained in a timely way or the individual would not reasonably be expected to withhold consent;

(b) The collection of the information is pursuant to a statute or regulation of Alberta or Canada that authorizes or requires the collection;

(c) The collection of the information is from a public body and that public body is authorized or required by an enactment of Alberta or Canada to disclose the personal information to the organization;

(d) The collection of the information is reasonable for the purposes of an investigation or a legal proceeding;

(e) The information is publicly available;

(f) The collection of the information is necessary to determine the individual's suitability to receive an honour, award or similar benefit, including an honorary degree, scholarship or bursary;

(g) The information is collected by a credit reporting organization to create a credit report where the individual consented to the disclosure to the credit reporting organization by the organization that originally collected the information;

(h) The information may be disclosed to the organization without the consent of the individual under section 20;

(i) The collection of the information is necessary in order to collect a debt owed to the organization or for the organization to repay to the individual money owed by the organization;

(j) The organization collecting the information is an archival institution and the collection of the information is reasonable for archival purposes or research;

(k) The collection of the information meets the requirements respecting archival purposes or research set out in the regulations and it is not reasonable to obtain the consent of the individual whom the information is about.

Your organization may use personal information about an individual without the consent of the individual if

(a) A reasonable person would consider that the use of the information is clearly in the interests of the individual and consent of the individual cannot be obtained in a timely way or the individual would not reasonably be expected to withhold consent;

(b) The use of the information is pursuant to a statute or regulation of Alberta or Canada that authorizes or requires the use;

(c) The information was collected by the organization from a public body and that public body is authorized or required by an enactment of Alberta or Canada to disclose the information to the organization;

(d) The use of the information is reasonable for the purposes of an investigation or a legal proceeding;

(e) The information is publicly available;

(f) The use of the information is necessary to determine the individual's suitability to receive an honour, award or similar benefit, including an honorary degree, scholarship or bursary;

(g) a credit reporting organization was permitted to collect the information under section 14(f) and the information is not used by the credit reporting organization for any purpose other than to create a credit report;

(h) The information may be disclosed by an organization without the consent of the individual under section 20;

(i) The use of the information is necessary to respond to an emergency that threatens the life, health or security of an individual or the public;

(j) The use of the information is necessary in order to collect a debt owed to the organization or for the organization to repay to the individual money owed by the organization;

(k) The organization using the information is an archival institution and the use of the information is reasonable for archival purposes or research;

(l) The use of the information meets the requirements respecting archival purposes or research set out in the regulations and it is not reasonable to obtain the consent of the individual whom the information is about.

Your organization may disclose personal information about an individual without the consent of the individual if

(a) a reasonable person would consider that the disclosure of the information is clearly in the interests of the individual and consent of the individual cannot be obtained in a timely way or the individual would not reasonably be expected to withhold consent;

(b) The disclosure of the information is pursuant to a statute or regulation of Alberta or Canada that authorizes or requires the disclosure;

(c) The disclosure of the information is to a public body and that public body is authorized or required by an enactment of Alberta or Canada to collect the information from the organization;

(d) The disclosure of the information is in accordance with a provision of a treaty that

(i) Authorizes or requires its disclosure, and

(ii) Is made under an enactment of Alberta or Canada;

(e) the disclosure of the information is for the purpose of complying with a subpoena, warrant or order issued or made by a court, person or body having jurisdiction to compel the production of information or with a rule of court that relates to the production of information;

(f) The disclosure of the information is to a public body or a law enforcement agency in Canada to assist in an investigation

(i) Undertaken with a view to a law enforcement proceeding, or

(ii) From which a law enforcement proceeding is likely to result;

(g) The disclosure of the information is necessary to respond to an emergency that threatens the life, health or security of an individual or the public;

(h) The disclosure of the information is for the purposes of contacting the next of kin or a friend of an injured, ill or deceased individual;

(i) The disclosure of the information is necessary in order to collect a debt owed to the organization or for the organization to repay to the individual money owed by the organization;

(j) The information is publicly available;

(k) The disclosure of the information is to the surviving spouse or adult interdependent partner or to a relative of a deceased individual if, in the opinion of the organization, the disclosure is reasonable;

(l) The disclosure of the information is necessary to determine the individual's suitability to receive an honour, award or similar benefit, including an honorary degree, scholarship or bursary;

(m) The disclosure of the information is reasonable for the purposes of an investigation or a legal proceeding;

(n) the disclosure of the information is for the purposes of protecting against, or for the prevention, detection or suppression of, fraud, market manipulation or unfair trading practices and the organization that is disclosing the information or to which the information is being disclosed is permitted or otherwise empowered or recognized under an enactment of Alberta or Canada or of another province of Canada to carry out any of those purposes;

(o) The organization is a credit reporting organization and is permitted to disclose the information under Part 5 of the *Fair Trading Act*;

(p) The organization disclosing the information is an archival institution and the disclosure of the information is reasonable for archival purposes or research;

(q) The disclosure of the information meets the requirements respecting archival purposes or research set out in the regulations and it is not reasonable to obtain the consent of the individual whom the information is about.

Schedule 4 – Notice Required When Sharing Personal Information With Other Organizations

Reference: *Sections 13(2) and 13(3) Personal Information Protection* Act

1) Before or at the time Personal Information about an individual is Collected from another organization with the Consent of the individual, you must notify the organization that is Disclosing the information that the individual has Consented to the Collection of the information.

(2) Before or at the time Personal Information about an individual is Collected from another organization without the Consent of the individual, you must provide the organization that is Disclosing the Personal Information with sufficient information about the purpose for which the Personal Information is being Collected to allow the organization that is Disclosing the Personal Information to make a determination as to whether their Disclosure of the Personal Information would be in accordance with PIPA.

Schedule 5 – Refusing Access

Reference: *Section 24 Personal Information Protection Act*

Your organization may refuse to provide access to Personal Information if

(a) The information is protected by any legal privilege;
(b) The disclosure of the information would reveal confidential information that is of a commercial nature and it is not unreasonable to withhold that information;
(c) The information was collected for an investigation or legal proceeding;
(d) The disclosure of the information might result in that type of information no longer being provided to the organization when it is reasonable that that type of information would be provided;
(e) The information was collected by a mediator or arbitrator or was created in the conduct of a mediation or arbitration for which the mediator or arbitrator was appointed to act

(i) Under an agreement,

(ii) Under an enactment, or

(iii) By a court;

(f) The information relates to or may be used in the exercise of prosecutorial discretion.

Your organization must not provide access to Personal Information if

(a) The disclosure of the information could reasonably be expected to threaten the life or security of another individual;

(b) The information would reveal personal information about another individual;

(c) The information would reveal the identity of an individual who has in confidence provided an opinion about another individual and the individual providing the opinion does not consent to disclosure of his or her identity.

If you are able to reasonably sever the personal information referred to above from the record, you must provide the individual with access to the remainder of the personal information in the record.

Definitions

In this document:

Collection

Collection means the act of gathering, acquiring, or obtaining *personal information* from any source, including third parties, by any means.

Consent

Consent is voluntary agreement with what is being done or proposed. *Consent* can be either express or implied or in some cases assumed. Express *consent* is given explicitly, either orally or in writing. Express *consent* is unequivocal and does not require any inference on the part of the organization seeking *consent*. Implied *consent* arises where *consent* may *reasonably* be inferred from the action or inaction of the individual.

Disclosure

Disclosure is making *personal information* available to others outside the organization.

Domestic

Domestic means related to home or family;

Employee

Employee means an individual employed by an organization and includes an individual who performs a service for or relation to or in connection with an organization

a. as an apprentice, volunteer, participant or student, or
b. under a contract or an agency relationship with the organization;

Investigation

Investigation means an investigation related to

a. a breach of an agreement
b. a contravention of an enactment of Alberta or Canada or of another province of Canada, or
b. 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.

Legal Proceeding

Legal proceeding means a civil, criminal or administrative proceeding that is related to

a. a breach of an agreement,
b. a contravention of an enactment of Alberta or Canada or of another province of Canada, or
c. a remedy available at law;

Organization includes

(i) a corporation,
(ii) an unincorporated association,
(iii) a trade union as defined in the *Labour Relations Code*,
(iv) a partnership as defined in the *Partnership Act*, and
(v) an individual acting in a commercial capacity,

but does not include an individual acting in a personal or domestic capacity;

Personal Employee Information

Personal employee information means, in respect of an individual who is an *employee* or potential *employee*, *personal information reasonably* required by the ***organization*** that is *collected*, *used* or *disclosed* solely for the purposes of establishing, not establishing, managing or terminating

a. an employment relationship, or
b. a *volunteer work relationship* between the ***organization*** and the individual but does not include *personal information* about the individual that is unrelated to the relationship;

Personal Information

Personal information is information about an identifiable individual, excluding an individual's name, title, and business address or business phone number.

Personal information does not include information of a personal nature that relates to an unidentifiable individual (i.e., a statistic).

Reasonable

What a reasonable person would consider appropriate in the circumstances.

Record

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

Sensitive Personal Information

Sensitive personal information includes information on medical or health conditions, financial information, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, sexual preferences, information related to offenses or criminal convictions.

Use

Use refers to the treatment and handling of *personal information* within the ***organization***.

Volunteer Work Relationship

Volunteer work relationship means a relationship between a service ***organization*** and an individual under which a service is provided for or in relation to or is undertaken in connection with the ***organization*** by an individual who is acting as a volunteer or is otherwise unpaid with respect to that service and includes any similar relationship involving the ***organization*** and an individual where, in respect of that relationship, the individual is a participant or a student.