



Information Privacy Rights

Under the *Personal Information Protection Act* (“PIPA”)

PIPA protects your “personal information” held by “organizations” in Alberta by establishing the rules for how organizations can collect, use or disclose personal information about their clients, customers and employees. These rules governing how organizations manage personal information, in effect, afford individuals with certain information privacy rights:

- Right to Consent**
- Right to Withdraw Consent**
- Right to Limitations on Collection, Use & Disclosure**
- Right to Protection of Personal Information**
- Right to Accurate Personal Information**
- Right of Access**
- Right to Correction**
- Right to Challenge Compliance**
- Right to Employee Privacy**

The purpose of this document is to educate individuals about those rights (for definitions, see the final section of this document). Relevant sections of PIPA are referenced in the left margin.

RIGHT TO CONSENT

- 7(1)(a),(c),(d) ▪ An organization cannot collect, use or disclose your personal information without your consent, except in very limited circumstances (outlined below).
- 7(1)(b) ▪ Generally, organizations must collect your personal information directly from you, unless you consent to having your personal information collected from another source. There are some exceptions.
- 7(2) ▪ An organization cannot, as a condition of supplying you with a product or service, require you to consent to the collection, use or disclosure of your personal information beyond what is necessary for it to provide you with that product or service.

Example: *It is not reasonable for a retailer to require that you provide your phone number when you make a cash and carry purchase. Of course, some of your personal information might be necessary to honour a warranty or to make a delivery.*

- 8(1)
8(2) ▪ Organizations can obtain your consent verbally or in writing. You are deemed to have consented if you voluntarily provide your personal information to an organization for a particular purpose, and it is reasonable to do so.

- 13(1)
- Before or at the time the organization collects your personal information, it must notify you of the *purposes* of the collection and offer you the name of someone in the organization who can answer your questions.

Example: *A prospective employer has your deemed consent to use your personal information to consider you for the job you applied for because you voluntarily submitted your résumé. However, the organization cannot use your address for a different purpose like forwarding your résumé to another employer. This would require a new consent from you.*

- 8(3)
- An organization can provide you with notice of its intention to collect, use or disclose your personal information, but must give you a reasonable opportunity to decline or object. If you do not respond, your consent is deemed.

Example: *When ordering a product online, the organization may use your address to send you the product you purchased, but it cannot use your personal information to send you other marketing material. However, when you are completing the online purchase order, the company can advise you that it will use your address to send you a catalogue unless you check the decline box.*

- 10
- An organization cannot obtain your consent by using false, misleading or deceptive practices or information.

EXCEPTIONS TO CONSENT

- 14
- An organization may collect, use or disclose your personal information *without* your consent, but only under the circumstances below.
 - **Collection without consent:**
 - it is clearly in your interests and timely consent cannot be obtained, or you would not reasonably be expected to withhold consent;
 - the collection is in accordance with other Alberta or federal legislation;
 - the personal information is collected from a public body that is authorized or required to disclose the information;
 - it is for an investigation or legal proceeding;
 - the information is publicly available;
 - it is necessary for an honour or award;
 - to create your credit report;
 - it is to collect a debt you owe to the organization, or to repay money owed to you; or
 - the collection is for research or archival purposes.

Examples: An insurance company does not require your consent to collect witness statements or other information regarding an investigation of your personal injury claim.

A company to whom you owe money does not require your consent to provide your personal information to a collection agency.

A law firm does not require your consent to gather your personal information in relation to a civil claim you are involved in.

17

▪ **Use without consent:**

- all of the instances mentioned previously under collection, and
- if the information is required to respond to an emergency that threatens life, health or security of the individual or public.

Examples: A car dealership does not need your consent to share your personal information with the manufacturer to use to contact you about a hazardous defect.

A collection agency hired to collect money you owe to another organization does not need your consent to use your personal information to contact you to collect the debt.

A company does not need your consent to use your phone number to make a sales call to you if your phone number is publicly listed.

20

▪ **Disclosure without consent:**

- all of the instances mentioned previously under collection and use;
- if it is in accordance with a treaty;
- to comply with a subpoena;
- to assist a public body or law enforcement agency in an investigation;
- to contact your next of kin if you are injured or die;
- it is to your surviving spouse or relative; and
- to protect against market manipulation or fraud.

Examples: Your landlord can disclose your name to police for their investigation into the burglary of your home that occurred while you were on vacation. Your consent is not required.

It is lawful for your employer to disclose your income-related information to the Canada Revenue Agency (CRA) without your consent.

A corporate official subpoenaed to a trial can disclose information about you without your consent in his or her testimony.

For more information on Consent, see PIPA Advisory 1 on the OIPC website.

RIGHT TO WITHDRAW CONSENT

- 9(1) You have the right to withdraw or vary your consent for an organization to collect, use or disclose your personal information, provided that it does not interfere with the performance of any legal obligations.
- 9(5) 9(6) Withdrawal of your consent may be given to the organization in the same manner in which you provided it.
- 9(2) 9(3) The organization is required to inform you of the likely consequences of withdrawing your consent (such as any services that can no longer be provided without your personal information), unless it is reasonably obvious.

Example: *You previously subscribed to a magazine. You can withdraw your consent to receive marketing material encouraging you to renew your subscription.*

RIGHT TO LIMITATIONS ON COLLECTION, USE & DISCLOSURE

- 11(1), 16(1), 19(1) An organization must collect, use and disclose your personal information only for purposes that are “reasonable”.
- 11(2), 16(2), 19(2) An organization must limit the collection, use or disclosure of your personal information to the extent that is reasonable to accomplish its purposes.

Examples: *It is not reasonable for your landlord to collect your Social Insurance Number (SIN) since it should only be required for income reporting and to manage national benefits and social programs. Also, if the landlord wishes to obtain your credit report, it can be obtained without your SIN using your name and date of birth.*

A prospective employer can use your personal information to consider you for the job you applied for, but cannot use your address for a different purpose like sending you marketing material for its products.

Although you gave your consent for your physiotherapist to disclose information about your treatment to your insurance company, the physiotherapist must limit disclosure to the injury being treated and refrain from disclosing information that is unrelated or about injuries from the past.

RIGHT TO PROTECTION OF PERSONAL INFORMATION

- 34 An organization must protect your personal information in its custody or under its control by making reasonable security arrangements against the risk of unauthorized access, collection, use, disclosure, copying, modification, disposal or destruction.

Examples: Your grocery store must ensure that copies of your credit card receipts are not accessible to employees who are not authorized to use or manage the information. The store should also ensure that receipts are shredded prior to disposal or that your credit card number is truncated on the printed receipts so that the information cannot be misused.

Your private educational institution must ensure that its computer system has reasonable technical defenses in place to protect course grades from being modified by hackers and that only staff members authorized to make changes have access to the system to do so.

For more information on Safeguards, see PIPA Advisory 8 on the OIPC website.

RIGHT TO ACCURATE PERSONAL INFORMATION

- 33
- An organization must make a reasonable effort to ensure that your personal information collected, used or disclosed is accurate and complete.

Example: Before reporting a payment default to a credit reporting agency, your credit card company must ensure that it has processed all payments received by the deadline and that it is applying the correct information to your credit profile rather than someone else's file.

RIGHT OF ACCESS

- 24(1) ▪ You have the right to request that an organization give you access to your personal information in its custody, explain how your personal information is being used, and to whom it was disclosed.
- 26(1) ▪ Your request must be made to the organization in writing.
- 28(1)(a) ▪ An organization must provide you with access to your records within 45 days of receiving your request.
- 31(1) ▪ There are circumstances in which it can extend the timeline.
- 32(1)
32(3) ▪ The organization can charge you a reasonable fee, but must give you an estimate first.
- 24(2) ▪ The organization must provide you with your personal information unless:
 - it is subject to legal privilege;
 - disclosure to you would reveal commercial or proprietary information;
 - it was collected for an investigation or legal proceeding;
 - giving you access might result in the organization no longer being given the information, or
 - it was collected by a mediator or arbitrator.

In such cases, the organization has discretion on whether to give you access.

- 24(3) ■ An organization is prohibited from giving you access to your personal information in cases where it could threaten someone's life or security, or if it would reveal someone else's identity that provided an opinion about you in confidence. An organization cannot give you access to someone else's personal information.
- 27(1) ■ An organization must make every reasonable effort to assist you in your application for access. The organization must respond accurately and completely, and explain any codes, terms or abbreviations used in your records.
- 29 ■ If you are refused access to all or part of your personal information, the organization must explain to you the reasons for the refusal, and the exception (described above) under PIPA on which the refusal is based.
- The organization must advise you who to contact at the organization if you have questions, and advise you of your right to request a review by the Commissioner.

For more information on Access, see PIPA Advisories 2, 3, 5, 6 and 7 on the OIPC website.

Example: *You put in a written request for access for your employee file with a former employer. You provide a signed and dated written request and are clear about which records you are seeking: your time sheets for 2005, training certificates, performance evaluations and documents pertaining to your severance package and layoff. Your former employer responds to you after 40 days and encloses the first three items, but advises in a covering letter that some records regarding your layoff were memos between the company and its lawyer, thus subject to legal privilege. Therefore these records were withheld from you under section 24(2)(a) of PIPA. The letter also explains that some of your performance appraisals have severed portions (blacked out) pertaining to clients who raised confidential concerns about you, pursuant to section 24(3)(c) of PIPA. The letter tells you who to call if you have questions and advises you that you contact the Commissioner if you are not satisfied with this response.*

RIGHT TO CORRECTION

- 25(1) ■ You have the right to request (in writing) that an organization correct an error or omission in your personal information in its custody.
- 25(2) ■ The organization must make that correction as soon as possible and send notice to any other organization to which your incorrect personal information was disclosed.
- 25(3) ■ If the organization decides not to make the correction, it must annotate your personal information with the correction you requested, but was not made.
- 25(5) ■ The organization cannot correct or alter opinions.

Example: You discovered that your life insurance company's records indicate that you have diabetes. Apparently, information about one of your parents has been mistakenly applied to you. You therefore send a written request asking for the information to be corrected and provide a copy of your recent lab result that demonstrates the absence of diabetes. The organization corrects your health status in all of its records, recalculates your premium and reissues your policy. It also notifies your insurance broker of the error and provides it with updated policy information.

For more information on Correction, see PIPA Advisory 4 on the OIPC website.

RIGHT TO CHALLENGE COMPLIANCE

- You have the ability to ask why an organization is collecting your personal information, how it will be used and to whom it will be disclosed.
- 5(3) ▪ You may direct your questions to the organization's Privacy Officer. PIPA requires that all organizations designate someone to be responsible for ensuring the organization is compliant with PIPA.
- 6 ▪ You may ask to see the organization's privacy policy to understand its practices. PIPA requires that all organizations develop and follow policies and provide information about those policies on request.
- 46(2) ▪ In the event that your concerns are not resolved by the organization, you can make a written complaint to the Commissioner about that organization's practices under PIPA.
- 46(1) ▪ Similarly, if you are not satisfied by the organization's response to your request for access to your personal information, you have the right to request the Commissioner conduct a review.

RIGHT TO EMPLOYEE PRIVACY

- You do not surrender your privacy rights in the workplace. However, those rights are different; not just for employees, but for volunteers as well.
- 15(2)(c)
18(2)(c)
21(2)(c) ▪ Rather than getting your consent an employer must notify you of its collection, use and disclosure practices ahead of time.
- Your employer can notify you of these practices verbally, in writing, by email, or by explaining its practices in company directives and policies that you are required to read.
- 15(2)(a)
18(2)(a)
21(2)(a) ▪ Of course, organizations' collection, use or disclosure of personal information must be reasonable for the purposes.
- 15(2)(b)
18(2)(b)
21(2)(b) ▪ The collection, use or disclosure must also be directly related to the employment relationship. In other words, it must be reasonably required to establish, manage or terminate the organization's employment relationship with you.

- This type of information is referred to as “personal employee information”. Anything not connected to the employment relationship is personal information, to which all the other rules discussed (such as consent) apply.

Examples: *Your employer has an online policy manual, the contents of which employees are required to be aware of. The policy explains that employee internet usage is monitored to ensure that employees adhere to the computer usage rules, which includes not visiting restricted websites. Later, the company sends out an email of its decision to start monitoring employee time usage of the internet, since employees don't have any reason to use the internet for more than an hour a day and there have been reports of serious abuse.*

You become injured and are claiming health benefits from your employer. The company sends you an information package which explains how your medical reports will be collected, used and disclosed and advises you that only the insurance provider will be aware of your specific diagnosis. Since only the insurance company decides whether you are eligible for medical benefits, your employer does not need to collect this information and only requires information about whether you are eligible and when you will return. When you return to work, the company explains that it will collect information about whether you are fit to return and whether any accommodations or restrictions apply. During your time off, your employer notifies you that the insurance company health workers will be disclosing your medical reports to another physician of your choice for an independent assessment.

DEFINITIONS

What is PIPA?

The *Personal Information Protection Act*, or “PIPA”, is an Alberta statute that governs how businesses operating in this province can collect, use or disclose the personal information of individuals. PIPA does not apply to federally-regulated organizations such as banks, airlines, telecommunications companies and railways. Those organizations are governed by federal privacy legislation.

What is an Organization?

An organization is a provincially-regulated private sector business operation in Alberta. This includes corporations, unincorporated associations, trade unions (under the *Labour Relations Code*), partnerships (under the *Partnerships Act*), as well as individuals who are acting in a commercial capacity [s.1(i)].

PIPA only applies to non-profit organizations in their commercial activities. Where there is no commercial activity involved, PIPA does not apply. This also means that PIPA does not apply to employees of non-profit organizations. To be considered a non-profit organization under

PIPA, the organization must be incorporated under the *Societies Act*, *Agricultural Societies Act*, or Part 9 of the *Companies Act*.

What is personal information?

Personal information is broadly defined as “information about an identifiable individual” [s.1(k)]. Information that might identify an individual or can be determined from the contents of the information is considered personal information. The actual contents of the information and the context in which it is disclosed may be factors that make it identifying information. If an individual cannot be identified, the information is not personal information.

Personal information also includes subjective information, such as an opinion, evaluation or comment. In privacy legislation, an individual’s personal views or opinions are generally considered to be that individual’s personal information, unless the views or opinions are about someone else. Views or opinions about another individual may also be the personal information of that other individual.

A subset of personal information is called “personal employee information” and it relates to individuals’ personal information reasonably required by an employer that is collected, used or disclosed solely for the purposes of establishing, managing, or terminating the employment or volunteer work relationship [s.1(j)].

This document was prepared to help organizations implement the Personal Information Protection Act (PIPA). This document is an administrative tool intended to assist in understanding PIPA. It is not intended as nor is it a substitute for legal advice. For the exact wording and interpretation of PIPA please read it in its entirety. This document is not binding on the Information and Privacy Commissioner of Alberta.

FOR MORE INFORMATION, CONTACT:

Office of the Information & Privacy Commissioner
#2460 – 801 6th Avenue SW
Calgary, Alberta T2P 3W2
(403) 297-2728 or 1-888-878-4044
Fax: (403) 297-2711
generalinfo@oipc.ab.ca

February 2007