Office of the
Information &
Privacy Commissioner
*for British Columbia*

Protecting privacy. Promoting transparency.



GUIDANCE DOCUMENT

# DEVELOPING A PRIVACY POLICY UNDER PIPA

MARCH 2019

# CONTENTS



# PURPOSE OF THIS GUIDANCE DOCUMENT

The *Personal Information Protection Act* (PIPA) requires organizations to develop and follow policies and practices to meet their obligations under PIPA, and to make these documents available on request.

PIPA applies to more than a million private sector organizations in British Columbia, including businesses, charities, associations, non-profits, and labour unions. Its purpose is to govern the collection, use, and disclosure of personal information by these groups. PIPA recognizes both the right of individuals to protect their personal information and the need of organizations to collect, use, or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.

Privacy policies describe how an organization handles personal information in a manner that is compliant with PIPA. They are an important resource for staff to follow. Privacy policies can also let individuals know how an organization handles personal information and what rights they have to access to that information. This document is designed to help you develop a privacy policy.

# WHAT IS PERSONAL INFORMATION

"Personal information" is a broadly defined term that includes information that is reasonably capable of identifying a particular individual either alone or when combined with information from other available sources. Personal information includes employee personal information.[1] It does not include business contact information[2] or work product information.[3]

Some examples of personal information are: name, address, gender, education, income, financial information, medical and genetic information, date of birth, drivers' license number, photographs or images of an individual, employment history, and product preferences.

# WHAT TO INCLUDE IN YOUR PRIVACY POLICY

Privacy policies should detail how your organization handles personal information. Organize your privacy policy in a way that best addresses your organization's privacy needs and risks. While you must address how you meet your obligations under PIPA, the level of detail involved may depend on the size of your organization, the quantity and type of personal information you handle, and the nature of those activities. The headings in this document are provided as guidance. They reference your obligations and are based on common privacy principles.

## Accountability

In this section, include a statement in your policy that your business is accountable for compliance with PIPA. Then:

- Define PIPA. For example: "BC's Personal Information Protection Act sets out rules for how organizations collect, use and disclose personal information."
- Provide a description of "personal information" under PIPA.
- Note that your organization is committed to being accountable for how you handle personal information, as well as how you follow the rules and procedures outlined in your policy.

## Identifying purposes & limiting collection

PIPA authorizes organizations to collect, use, and disclose personal information only for purposes that a reasonable person would consider appropriate in the circumstances and if your organization has received consent or is authorized to collect without consent. Your policy should explain the following:

---

[1] Information collected, used or disclosed solely for the purposes reasonably required to establish, manage or terminate an employment relationship between the organization and an individual

[2] Information used to contact an individual at their place of business for a purpose related to that business.

[3] Information prepared or collected by an employee as part of that individual's work responsibilities.

- Your organization will only collect, use, or disclose personal information that is necessary to fulfill the purpose of the collection.
    - Collect only the minimum amount of personal information required to achieve the purpose for the collection.
- The types of personal information you collect.
    - Use real examples.
- All of the purposes for collecting personal information.
    - Examples of the purpose for the collection might include: to verify identity, to verify credit-worthiness, to provide requested services or products, or to enrol an individual in a program.

## Consent

PIPA requires businesses to get consent for the collection, use, or disclosure of personal information about an individual, unless otherwise permitted by the Act. This means that, except for limited circumstances, you must tell individuals how their personal information will be collected, used, or disclosed, either before or at the time of collection. This section of your privacy policy should explain:

- that your business will get individuals' consent to collect, use, or disclose their personal information, except where you are legally authorized or required by law to do so without consent.[4]
- how you will obtain consent, including:
    - how you will notify individuals of the purpose for collecting their personal information;
    - that individuals can consent orally, in writing or electronically; and
    - that consent may be implied or express, depending on the nature and sensitivity of the personal information.[5]

[4] If there are any situations where your organization may collect, use or disclose personal information without an individual's knowledge or consent—as allowed under PIPA sections 12, 15 and 18—you should say so and list them specifically.

[5] When determining type of consent, such as express, deemed or opt-out consent, consider both the sensitivity of the personal information and what a reasonable person would deem appropriate. Express consent occurs when an individual, knowing what personal information is being collected and for what purposes, willingly agrees to his or her personal information being collected, used and disclosed as notified. Express consent can be given in writing or verbally. Implied consent happens when an individual doesn't expressly give consent, but volunteers information for an obvious purpose and a reasonable person would consider it appropriate in the circumstances. Opt-out consent is consent by not declining consent. For example, a form notifying an individual of the organization's intended use of the personal information with a "check-off" box. Individuals can check the box if they do not want the business using their information for this purpose.

- that consent will not be required beyond what is necessary to provide a product or service.
- that individuals may withdraw consent at any time by giving your business reasonable notice, unless withdrawing consent would frustrate your performance of a legal obligation (such as a contract between the individual and your organization);
    - PIPA requires you to tell individuals of the likely consequences of withdrawing consent (such as being unable to provide them with services or goods that require the collection of their personal information).
- that you can collect, use, or disclose employee information without consent if it is reasonable for the purposes of establishing, managing, or terminating an employment relationship between your organization and the individual.

## Limiting use and disclosure

PIPA limits the use and disclosure of personal information to purposes that a reasonable person would consider appropriate in the circumstances and where your organization has either received consent or is authorized to collect without consent. Your privacy policy should set out the limits on its use, disclosure, and retention of personal information by explaining:

- that you will not collect, use, or disclose personal information except for the identified purposes for collection, unless you have received additional consent or the processing is authorized without consent;
- that you will disclose personal information where authorized by PIPA or required by law (for example, in the event of a court order, subpoena, or search warrant); and
- any other circumstances for which your organization discloses personal information.
    - If you retain another organization to do work for you that involves personal information, explain that you will ensure there is an agreement in place that ensures this organization understands and follows the same PIPA obligations.

| | |
|---|---|
| **ADVICE FROM THE COMMISSIONER** | **Review your privacy policies on a regular basis to ensure they reflect the current practices of your organization in meeting your obligations under PIPA.** |
| | **Review your organizational practices to ensure they are compliant with privacy policies.** |
| | **Ensure everyone within your organization who handles personal information is aware of and understands your privacy policies.** |

## Retention

PIPA requires you to retain personal information used to make decisions that directly affect individuals. Your organization must destroy the personal information once it is no longer in use for the purpose it was collected unless it is necessary to retain the information for legal or business purposes. Your policy should explain that:

- you will keep personal information used to make a decision that directly affects individuals for at least one year after you make that decision; and
- after that period of time has passed, you will securely destroy or anonymize personal information once it is no longer necessary to fulfil the identified purposes or any other legal or business purposes.
    - Be as specific as you can about how long your organization will retain personal information.

## Accuracy

You are required under PIPA to make reasonable efforts to ensure that personal information collected is accurate and complete, if the information is likely to be used in decisions that affect individuals or to be disclosed to another organization. Your policy should explain that:

- your organization will make reasonable arrangements to ensure that the personal information you collect, use, or disclose is accurate and complete;
- individuals may request that your organization correct any errors or omissions in their personal information that is under your organization's control;
- if your organization is satisfied that an individual's request for correction is reasonable, you will correct the information and send the corrected information to organizations you disclosed that information to during the year before the date the correction was made; and
- if your organization is not satisfied that the request for correction is reasonable, you will annotate the information, noting that the correction that was requested but not made.

## Safeguards

PIPA requires you to protect personal information under your control by making reasonable security arrangements to prevent unauthorized access, collection, use, disclosure, copying, modification, disposal, or similar risks. You must ensure your business has appropriate security controls in place to reasonably protect personal information from things like snooping, hacking, theft, loss, tampering, and copying of the information when not authorized. What is reasonable can depend on the volume and sensitivity of the information. Your policy should explain:

- the administrative[6], physical[7] and technological[8] security safeguards used to protect personal information; and
- the process for responding to suspected privacy breaches, so that your staff know what to do and who to talk to in the event of a breach.

## Individual access

PIPA allows individuals to request access to their own personal information that is under your control. Your policy should detail how individuals can access their personal information by explaining that:

- individuals have the right to access:
    - their personal information;
    - information about the ways in which their personal information is or has been used; and
    - the names of the individuals and organizations to which their personal information has been disclosed;
- a request for access must be made in writing;
- individuals may be required to prove their identity before you give them access to their personal information;
- you may charge a "minimal" fee for providing an individual with access to their personal information. If a fee is required, your organization will give the individual a written fee estimate in advance;
    - Your business may require payment of a deposit or the whole fee before releasing the requested information.
- you will provide requested personal information within 30 business days after it is requested, unless a time extension is granted under PIPA; and
- if your business is authorized or required by PIPA to refuse access, you will tell the applicant in writing, stating the reasons for your refusal and outlining further steps that are available to the applicant.

---

[6] Administrative security controls are operational procedures and mechanisms implemented primarily by individuals within the organization to ensure proper handling of personal information, as opposed to through the use of automated systems or physical measures (i.e., policies, training, compliance monitoring, internal audit).
[7] Physical security controls are measures that utilize physical restrictions to limit access to personal information by unauthorized individuals (i.e., locked cabinets or rooms, alarm systems, security personnel).
[8] Technological security controls are for protecting personal information held in computer systems (i.e., passwords, encryption, firewalls, restricting electronic access).

## Challenging compliance

PIPA requires you to develop processes for responding to complaints that may arise. Individuals need to know how they can ask questions about the handling of their personal information. Your policy should provide:

- information about how an individual can make a complaint, such as by telephone or in writing;
    - Individuals may be required to prove their identity before discussing any complaint or request that involves their personal information.
- contact information for the person in your organization who is responsible for compliance with PIPA; and
- contact information for the Office of the Information and Privacy Commissioner, if an individual is not satisfied with how your organization performs its duties under PIPA, or to seek a review of your organization's response to their access or correction request.

## Openness

PIPA requires businesses to develop these policies and practices and to make this information available upon request. While it is not a requirement under PIPA, the easiest ways to share your privacy policies are to use them in your employee training and to post them on your website.