



Service Providers Outside Canada: Notification, Policies and Practices

Personal Information Protection Act Information Sheet 12

Introduction

Organizations in Alberta operate in an increasingly global business environment. Large and small businesses now enter into arrangements for specialized services that are provided, directly or indirectly, by businesses in other countries. Information technology has enabled organizations to take advantage of business options that enhance their services to clients while reducing costs. At the same time, organizations have found it necessary to address concerns about the risks to privacy associated with outsourcing, in particular, the protection of personal information and the disclosure requirements under foreign laws.

The *Personal Information Protection Amendment Act, 2009* makes a number of amendments designed to foster openness and accountability in private-sector organizations with respect to the use of service providers outside Canada; the Amendment Act comes into force on May 1, 2010. This Information Sheet explains the Act's new provisions for notification and for policies and practices with respect to service providers outside Canada in the context of the existing requirements.

Privacy principles relating to notification, policies and practices

Most privacy laws are based on a number of common principles. One of the most fundamental is the principle of openness, the principle that an organization should explain to individuals its policies and practices with respect to their personal information. This principle is closely related to the principle that an organization should inform individuals about the purposes for which it is collecting personal information at the time of the collection and that the use of the information should be limited to fulfilling those purposes. In both cases, it is generally understood that information should be available without unreasonable effort on the part of the individual and in a form that is generally understandable.

The provisions in PIPA respecting notification (sections 13 and 13.1) and policies and practices (section 6) are based on these principles.

Notification respecting the collection of personal information

Section 13(1) of the Act is the general provision for notification.

Notification required for collection

13(1) Before or at the time of collecting personal information about an individual from the individual, an organization must notify that individual in writing or orally

(a) as to the purposes for which the information is collected, and

(b) of the name or position name or title of a person who is able to answer on behalf of the organization the individual's questions about the collection.

Section 13(1) requires an organization to inform the individual of the purposes for which the individual's personal information is being collected. This requirement applies only when an organization is collecting personal information *directly from the individual*.

An organization is not required to provide notification to the individual when the organization is authorized to collect the individual's personal information from another person (e.g. a landlord can collect personal information about a tenant from the tenant's neighbour, without the tenant's consent, and without notification, to investigate a breach of a lease).

An organization is also not required to provide notification if an individual's consent to the collection of his or personal information is "deemed" (section 13(4)). An individual's consent is deemed (or implied) when the individual voluntarily provides information to the organization and it is reasonable to do so. For example, an individual may volunteer a credit card to make a payment. The Act considers the individual to have given implied consent to the use of the credit card information to process the payment. Notification is not required because the purpose is obvious. However, an organization would have to obtain express consent and provide notification if the organization was collecting the information for an additional purpose that was not obvious (e.g. to create a customer list for marketing).

An organization should define the purposes for collecting personal information as clearly and narrowly as possible so the individual can understand how the organization will use or disclose the information. Some purposes for which an organization might collect personal information include opening an account, registering a warranty and guaranteeing a travel reservation.

Notification must be given before or at the time the personal information is collected and may be given in writing or orally. There are many ways of providing notification. For example, an organization may provide notification in writing by including information about the purpose of collection on a form (print or electronic) that is used to collect the information. Notification may be provided orally when collecting personal information during a phone call. (Organizations notifying individuals orally may find it advisable to use a script and to have the staff member record that the notice was given. A clear practice regarding oral notification can be helpful in the case of any misunderstanding.)

When giving notification, the organization must provide contact information for a person who can answer questions about the collection of personal information. The person in this role should be someone who is knowledgeable about the organization's purpose for collecting the information. The contact information can include the person's name or position title (using the position title on forms may assist in reducing the need for updating).

An organization has a positive duty to provide notification under PIPA. The Information and Privacy Commissioner has noted that notification cannot be inferred (PIPA Order P2006-008).

Notification respecting service providers outside Canada

Section 13.1 establishes a *new* duty to notify, in addition to the general requirement under section 13. Where an organization uses a service provider outside Canada to collect, use or disclose personal information, section 13.1 requires the organization to notify individuals as to how they can obtain information about the organization's policies and practices with respect to the service provider.

Notification respecting service provider outside Canada

13.1(1) Subject to the regulations, an organization that uses a service provider outside Canada to collect personal information about an individual for or on behalf of the organization with the consent of the individual must notify the individual in accordance with subsection (3).

(2) Subject to the regulations, an organization that, directly or indirectly, transfers to a service provider outside Canada personal information about an individual that was collected with the individual's consent must notify the individual in accordance with subsection (3).

(3) An organization referred to in subsection (1) or (2) must, before or at the time of collecting or transferring the information, notify the individual in writing or orally of

(a) the way in which the individual may obtain access to written information about the organization's policies and practices with respect to service providers outside Canada, and

(b) the name or position name or title of a person who is able to answer on behalf of the organization the individual's questions about the collection, use, disclosure or storage of personal information by service providers outside Canada for or on behalf of the organization.

(4) The notice required under this section is in addition to any notice required under section 13.

"Service provider" means any organization, including, without limitation, a parent corporation, subsidiary, affiliate, contractor or subcontractor, that, directly or indirectly, provides a service for or on behalf of another organization (**section 1(1)(m.3)**)

A "parent corporation" is a corporation that controls another corporation (*Dictionary of Canadian Law*).

A "subsidiary" is a corporation which, in respect of another corporation, is controlled, either directly or indirectly, by that other corporation (*Dictionary of Canadian Law*).

An "affiliate" is a corporation that is related to another corporation by shareholdings or other means of control; a subsidiary, parent, or sibling corporation (*Black's Law Dictionary*).

It is important to note that the term “service provider” is not limited to an organization providing services under contract with the principal organization; a service provider may be a subcontractor. A service provider may also be a parent corporation, a subsidiary or an affiliate. A service provider would not include an employee located in another country or an employee travelling on business.

There are no regulations relating to section 13.1.

► **Circumstances in which notification is required – collecting personal information**

Section 13.1(1) requires an organization to notify an individual if a service provider outside Canada will *collect* the individual’s personal information on behalf of the organization. This requirement applies only when the organization is collecting the personal information with the individual’s consent. If the organization is collecting personal information without consent (and is authorized to do so under section 14 of PIPA), the organization is not required to notify the individual.

For example, a retail business that sells computers may offer its customers a technical support service that provides assistance online or by telephone from another country. Since the service provider outside Canada would have to collect some customer personal information, the retail business would be required to notify the customer. On the other hand, an organization taking legal action against an individual, and using the legal services of a parent corporation in another country to do so, would not be required to notify the individual about the collection of the individual’s personal information. Consent for the collection of information related to the legal action is not required, so notification is not required.

► **Circumstances in which notification is required – transferring personal information**

Section 13.1(2) requires an organization to notify an individual if the organization *transfers* the individual’s personal information – directly or indirectly – to a service provider outside Canada. This requirement applies only where the individual originally gave the principal organization consent for the collection of his or her personal information. Section 13.1(2) applies even if the organization does not transfer the personal information *directly* to the service provider.

For example, an organization may contract with a business that provides a suite of business services, such as accounts, collections and customer relationship management. That business subcontracts for some services with a service provider based in India and transfers the personal information to India for the purpose of providing those services. The principal organization would be required to notify individuals whose personal information will be transferred to the service provider in India.

On the other hand, if the local contractor allows the subcontractor’s employees in India to access the information online but not to store it in India, the principal organization would likely not be required to provide notification. For practical purposes, this arrangement would not involve the transfer of any personal

information to India; all the information would remain in Canada.

The following are some circumstances where **notification is not required**.

- Transmission of information through an internet service provider (ISP).
Section 13.1 applies only where there is a collection of personal information *on behalf of the organization* by a service provider outside Canada, or where there is a transfer *to a service provider*. An ISP is not collecting personal information on the organization's behalf. Nor is the information being transferred to the ISP.
- Transfer of credit card information to a customer's credit card company.
A credit card company is not the organization's service provider. The customer has entered into a relationship with the credit card company, which is collecting the personal information on its own behalf.
- Personal employee information that is collected, used or disclosed without consent in accordance with PIPA's provisions for employee information.
Notification under section 13.1 is required under the Act only when personal information is collected with the individual's consent.

If an organization contracts with a business that subcontracts with a service provider outside Canada to collect, use or disclose personal information on behalf of the organization, the organization may find it helpful to include contract clauses requiring the business to give the organization the right to approve the use of a service provider outside Canada, or to obtain the organization's approval for any change to a service provider outside Canada. To ensure the organization's compliance with PIPA, the contract should at least require the business to inform the principal organization when it changes from a subcontractor in one country to a subcontractor in another country.

It should be noted that PIPA will *not* require an organization to obtain the individual's *consent* to its use of a service provider outside Canada.

► **What information must be included in the notification**

If section 13.1(1) or (2) applies to an organization, that organization must notify the individual in accordance with section **13.1(3)**.

The information to be provided in the notice to the individual is fairly minimal. The notification

- should indicate that the organization uses a service provider outside Canada to collect or process personal information for a specified purpose,
- must state how the individual can access written information about the organization's policies and practices regarding service providers outside Canada (e.g. provide a website address),
- must provide contact information for a person who can answer the individual's questions about the collection, use, disclosure or storage of personal information by the service provider outside Canada.

The contact person should be able to inform an individual about the location of the service provider and, in general terms, how personal information is collected, used, disclosed or stored, as the case may be, for the purpose for which the individual's personal information was collected by the organization. The contact person should be able to answer questions that are reasonably specific to the individual's relationship with the organization. The contact person would not be expected to provide details of the laws governing the disclosure of personal information in the service provider's country.

► **How notification may be given**

The organization subject to PIPA is responsible for ensuring that notification is provided, but notification may be given by a contractor, including the service provider outside Canada, as long as the notification is given before or at the time an individual's personal information is collected by or transferred to the service provider.

Notification may be given in writing or orally. For example, a notification for a new collection of personal information by a service provider outside Canada could be

- provided on a form (print or electronic) used to collect personal information, or
- given in a recorded message before an individual is connected with the service provider for the collection of the individual's personal information.

A notification regarding the transfer of personal information to a service provider outside Canada could be given at the time of the original collection.

If notification regarding a transfer is not given at the time of the original collection, or if an organization decides to transfer the personal information to a service provider outside Canada *after* the original collection of the personal information, the organization may be able to provide the notification when it is communicating with the individual on other matters. For example, the organization could provide the notification

- with a customer's regular statement,
- with a subscriber newsletter, or
- by e-mail (if the organization normally communicates with the client by e-mail).

Policies and practices

The provision in PIPA for policies and practices (section 6) supports the principle that organizations that collect, use and disclose the personal information of clients, as well as employees, should be open about their policies and practices regarding the protection of that personal information. As amended, section 6 includes new provisions regarding service providers outside Canada.

Policies and practices

6(1) An organization must develop and follow policies and practices that are reasonable for the organization to meet its obligations under this Act.

(2) If an organization uses a service provider outside Canada to collect, use, disclose or store personal information for or on behalf of the organization, the policies and practices referred to in subsection (1) must include information regarding

- (a) the countries outside Canada in which the collection, use, disclosure or storage is occurring or may occur, and
- (b) the purposes for which the service provider outside Canada has been authorized to collect, use or disclose personal information for or on behalf of the organization.

(3) An organization must make written information about the policies and practices referred to in subsections (1) and (2) available on request.

PIPA requires an organization to turn its attention to the way the Act applies to the personal information it collects. The Act requires an organization to develop and follow policies and practices that are reasonable for the organization to meet its obligations under this Act. An organization's policies and practices should address matters that arise regularly in the course of the organization's business.

In most cases, an organization will have internal policies and practices that employees have to follow when performing business functions (e.g. opening an account for a client). It is generally not helpful, either for the organization or the client, to make internal policies available to clients. Organizations generally choose to develop a policy document for clients that focuses on matters of particular interest to clients.

A model privacy policy, developed by Access and Privacy, Service Alberta, with small businesses in mind, is available at <http://pipa.alberta.ca/resources/doc/PerInfoProtectPolicy.doc>

The policy is designed for client personal information. Most organizations find it practical to have a separate policy for employee personal information.

The model policy can be adapted to an organization's needs. It is important to remember that PIPA requires an organization to *follow* its policies and practices. So a policy for clients must represent an organization's actual practices. The standard, as throughout PIPA, is to have policies and practices that are *reasonable* for meeting statutory obligations.

► **Policies and practices respecting service providers outside Canada**

An organization may decide to incorporate the required information respecting services providers outside Canada into a general policy document or have a policy document that addresses service providers outside Canada separately. The following comments discuss what must be included with respect to service providers, whether within a general policy document or a separate document relating to service providers outside Canada.

The first requirement is that an organization that uses a service provider outside Canada to process personal information must provide information regarding *the countries outside Canada in which the collection, use, disclosure or storage of personal information is occurring or may occur.*

The wording is intended to provide some flexibility for organizations that change service providers frequently and for organizations that use service providers in more than one country. At the same time, it is intended that a policy should explain the organization's practices in ways that are meaningful to individuals.

For example, if an organization contracts with a business in Alberta that outsources certain data processing, such as account applications, to India and Argentina, it would be reasonable to state that the processing of account applications may occur in either of those countries. However, if applications for new accounts are routinely processed in one country and account enquiries are handled in another country, it would be reasonable to say this.

It should be noted that the policy needs to address the storage of personal information by a service provider outside Canada (for any purpose, including back-ups).

The second requirement is that an organization that uses a service provider outside Canada to process personal information must provide information regarding *the purposes for which the service provider has been authorized to collect, use or disclose personal information for or on behalf of the organization.*

Informing individuals about the purposes for which service providers outside Canada are authorized to collect, use or disclose personal information is likely to require more detail than informing individuals about the purposes for which an organization is collecting personal information.

For example, a section in a policy relating to an organization's purposes for collecting personal information might explain that an organization collects personal information *for the purpose of operating a loyalty program.* A section in a policy respecting the use of service providers outside Canada might need to be more specific, stating, for example, that personal information is transferred to a service provider in the United States *to process customer transaction information for the purpose of keeping the customer's loyalty program account up to date.*

An organization is not required to provide information about any possible disclosure by a service provider that is *not* authorized by the organization and over which the organization would have no control, such as a law compelling the production of records for a law enforcement purpose.

As with policies and practices generally, an organization is not required to make its internal policies and practices for managing its business relationships, including information about contracts with service providers, available to clients.

Although an organization is not required to make business information about its contracts available to clients, an organization may choose to include in its policy

for clients a statement that the organization is responsible for the service provider's compliance (PIPA section 5(2)). Also, the organization may choose to let clients know that the organization uses contractual or other means to provide a comparable level of protection to personal information that is collected by, or transferred to, the service provider.

For most organizations, the most convenient and cost-effective way to provide current information about policies and practices is to post the information on the organization's website. It is considered a good practice to have a clear link to this information from every page. The organization should have a process for regularly reviewing and updating information about policies and practices.

Other resources *Personal Information Protection Policy for Small and Medium-Size Businesses*

Publications are available on-line from:

Access and Privacy
Service Alberta
pipa.alberta.ca

The website of the Office of the Information and Privacy Commissioner also contains resources, at www.oipc.ab.ca.

This Information Sheet was prepared to assist organizations that are subject to the *Personal Information Protection Act*. This document is an administrative tool intended to assist in understanding the Act. It is not intended as, nor is it a substitute for, legal advice. For the exact wording and interpretation of the Act, please read the Act in its entirety. This Information Sheet is not binding on the Office of the Information and Privacy Commissioner of Alberta.