

Hand Over the Information – It’s Mine, It’s Personal

On January 1, 2004, non-profit organizations in Alberta became subject to Alberta’s *Personal Information Protection Act* (PIPA). PIPA is Alberta’s response to PIPEDA – the *Personal Information Protection and Electronic Documents Act*. This federal legislation specifies how private sector organizations may collect, use, or disclose personal information in the course of commercial activities. This federal act was approved in the spring of 2000 and came into effect in stages. It currently covers federally regulated private sector organizations. Public sector organizations have been under similar coverage for years.

On January 1, 2004, PIPEDA extended to every organization that collects, uses or discloses personal information in the course of a commercial activity within a province. But if a province adopts legislation that is substantially similar to PIPEDA – in Alberta’s case PIPA – the organizations, classes of organizations or activities covered by the provincial legislation are exempt from the application of PIPEDA.

PIPA creates rules about collecting, using, and disclosing (showing, telling or giving some other organization) personal information to balance:

- an individual’s right to have his or her personal information protected, and
 - an organization’s need to collect, use or disclose personal information for purposes that are reasonable, that is, for legitimate business purposes.

The Act also gives individuals the right to ask an organization to show them the personal information it has about them and to ask for the information to be corrected if they think a mistake has been made.

Why Is There A Need For These Laws Now?

These laws are part of similar legislative activity around the world, but particularly resulting from two pressures: market concerns and pressure from the European Union. For the past two decades, it has become evident that cheap, powerful, and easily available computers made data collection, duplication, processing, and transfer possible in a way that subjected consumers to privacy invasion, identity theft, and fraud, with a particular concern about electronic commerce.

In Europe, early legislation enshrined a principle that required key sectors — particularly the financial — to only deal with countries that had standards at least as vigorous as those of the European Union. In turn, Canada examined its relations with its own citizens, and the standards and trade patterns with Europe in coming to develop PIPEDA.

What personal information is covered by PIPA?

Personal information is information, recorded or not, about an identifiable individual. For example, it includes:

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

The definition of personal information does not include business contact information. This covers information normally found on a business card, such as job titles, business telephone numbers (office, cell or fax), business address, and e-mail.

In Europe, early legislation enshrined a principle that required key sectors — particularly the financial — to only deal with countries that had standards at least as vigorous as those of the European Union.

What Does PIPA Require Organizations Collecting Personal Information to Do?

In general terms, a collecting organization to which PIPA applies is required to do the following:

- Obtain consent for collecting, using, and disclosing personal information, except when inappropriate (for example, in an emergency or when consent would compromise the availability or accuracy of the information). Obtain the consent in a form appropriate to the kind of information concerned. If an individual modifies or withdraws his or her consent, respect the changes.
- Collect personal information only for reasonable purposes and only as much as is reasonable for those purposes. Except when inappropriate, collect personal information directly from the individual concerned and inform the individual of how you will use and disclose the information.
- Use and disclose personal information only for the purposes for which it was collected, unless the individual consents or the Act permits the use or disclosure without consent.
- On request, provide an individual with information about the existence, use, and disclosure of the individual's personal information and provide access to that information, if reasonable. On request, correct information that is inaccurate.
- Ensure that any personal information is as accurate as necessary for the collection purposes; ensure that personal information is secure; and keep the information only as long as reasonable for business and legal reasons.
- Designate an individual to make sure you comply with the Act and make information about the organization's management of personal information available on request (from the Office of the Information and Privacy Commissioner's publication *The Personal Information Protection Act On a Page*)

What About Non-Profits?

The Act contains a provision that limits the application of the Act to only certain personal information held by some kinds of non-profit organizations. Non-profit organizations will become subject to the Act when they collect personal information as part of a commercial activity. For example, the Act will apply when a non-profit organization registers individuals in a course or provides services for a fee, such as counselling or babysitting services. Another example would include the sale of goods that involves the collection of personal information, such as by mail order. A non-profit organization includes an organization registered under the *Societies Act* or the *Agricultural Societies Act*, or Part 9 of the *Companies Act*. Non-profit organizations that do not carry out commercial activities will not be subject to the Act. For non-profit organizations, the Act applies only to commercial activities involving the handling of personal information, including the sale of donor or membership lists. It does not apply to personal employee information.

The question arises whether an organization must get consent to use personal information collected before January 1, 2004? This kind of personal information may be used for the purposes for which the information was collected. The Act will deem that consent was provided for the collection of the information, and it could be used and disclosed for purposes for which it was collected. Once the Act comes into force, it will be treated the same as information collected after January 1, 2004. For example, if an individual provided their name and mailing address in order to receive a catalogue, the business may continue to use that information to send out catalogues. If the business wants to use the contact information for a new purpose, then a new consent will be required.

What should A Non-Profit Do?

1. Have someone made responsible for dealing with your organization's initial treatment under PIPA.
Have your organization's responsible person read the Act:
<http://www.oipc.ab.ca/pipa/act.cfm>
2. Have them read *Information Sheet 1: Non-Profit Organizations*, describing how Act will apply to non-profit organizations in Alberta.
<http://www.psp.gov.ab.ca/publications.html>
3. Have the person responsible determine whether

The question arises whether an organization must get consent to use personal information collected before January 1, 2004? This kind of personal information may be used for the purposes for which the information was collected.

- (i) your organization is incorporated under the *Societies Act* or the *Agricultural Societies Act*, or registered under Part 9 of the *Companies Act*? If not, then the entire Act applies to the organization's activities.
 - (ii) the activities undertaken by your organization involve the collection, use or disclosure of personal information within Alberta?
 - (iii) the activities involving the collection, use or disclosure of personal information meet the definition of a commercial activity?
6. If your organization carries on commercial activities outside Alberta, visit http://www.privcom.gc.ca/index_e.asp
7. Have the person responsible for reviewing this information prepare a report for the Board.
8. In reviewing the report and determining how best to respond, the Board should consider how PIPA (and possibly PIPEDA) applies and consider the following matters.
 - (i) appointing a Compliance Officer;
 - (ii) conducting a privacy audit and whether, depending on the nature of information held by the organization whether provision should be made for regular internal or external compliance audits;
 - (iii) developing a list of approved purposes for collection of personal information;
 - (iv) preparing privacy policies, brochures and consent forms, including:
 - (a) Ensuring each individual's consent, for each database and purpose;
 - (b) that all uses of, or disclosures from, each database are properly recorded, protected, and are in accordance with the purposes; and
 - (c) reviews of the databases for accuracy in accordance with the sensitive nature of the information.
 - (v) consider a new filing system that separates personal information;
 - (vi) consider how to maintain compliance including developing a response plan in the event of allegations of a privacy breach.
9. The Board should revisit its initial consideration about PIPA at least once a year.

Laird Hunter is a lawyer with the firm of Worton Hunter & Callaghan in Edmonton, Alberta.

This column has been sponsored by:

Alberta
COMMUNITY DEVELOPMENT

Libraries, Community and
Volunteer Services
Board Development Program