TEN STEPS TO IMPLEMENT PIPA

Alberta's *Personal Information Protection Act* (PIPA) sets out the rules for handling the personal information of an organization's customers and employees. The Act came into effect in Alberta on January 1, 2004.

In the Act, organizations include corporations, unincorporated associations, trade unions, partnerships, and individuals running their own businesses. There are special rules that apply to non-profit organizations and self-governing professional organizations. PIPA does not regulate the collecting, using, or disclosing of personal information for domestic, artistic, literary, or journalistic purposes.

To implement the Act on private sector privacy, follow these steps.

1. Put Someone in Charge

Put someone in charge with enough authority and resources to do the job. This employee would be the contact for the public and employees when privacy issues arise.

You may want to assign other staff to help prepare the organization for the Act. A team is likely more effective since areas such as information technology, records management, legal services, human resources and operations will be affected.

2. Become Familiar with the Act

The staff working on privacy matters will need to be familiar with the Act.

3. Review How Your Organization Handles Personal Information

Look at how you handle personal information in the organization, from when it is collected to when it is destroyed. Ask these questions:

- What personal information do we collect? Is any of it particularly sensitive information?
- Why do we collect it?
- Are individuals likely to be aware that we collect this information? Do they know why it is collected?
- How do we collect it? Does it come from the individual at the cash register, a form, a survey, loyalty program, or online transaction? Is any personal information collected by a contractor located outside Canada, on our behalf?
- What do we use it for? Where do we use it?

Office of the Information and Privacy Commissioner of Alberta

Updated JANUARY 2018
Published in 2004 and 2010 with Service Alberta

- Who is it disclosed to? Does the organization contract out any functions or activities involving personal information? Does it go to any business partners?
- Where do we keep it? Is it stored in one place or in several places? Is personal information transferred to another country for processing or storage?
- How is it secured?
- Who has access to or uses it? Who needs to have access?
- When is it disposed of? How is it disposed of?
- Do we have a process in place to deal with security breaches?

4. Put Your Practices to the Test

Consider whether your organization's information handling processes measure up against the Act. Develop a plan to overcome any deficiencies, starting with the most problematic areas. These include your handling of the most sensitive personal information collected or of the most vulnerable to improper use or disclosure.

5. Develop Privacy Policies and Practices

Consult the staff that handles personal information when developing privacy policies and practices to comply with the Act. Written information on these policies must be available to the public on request.

Consider policies and practices in the following areas:

- Protecting employee and customer personal information, and ensuring its accuracy, storage, and disposal.
- Ways to obtain and record consents, and handling withdrawals of consent.
- Ways to record uses and disclosures of personal information.
- Ways to keep information as accurate as is needed for decision-making.
- Adequate security measures to protect personal information, including information on- site, with staff traveling for business, or in the custody of contractors.
- If service providers outside Canada are used to collect, use, disclose or store personal information, the countries in which those service providers are located, and the purposes for which the service providers are authorized to collect, use or disclose personal information.
- Developing keep-and-destroy procedures so you can destroy personal information no longer required in a secure manner.

6. Train Staff

Ensure you adequately train staff for their responsibilities. Training may cover such areas as:

- The principles of privacy protection.
- The organization's policies and practices.
- How the Act affects their specific job and the personal information they handle or are responsible for.
- How to handle or redirect questions received under the Act.
- What to do in the event of a security breach.

7. Develop an Access and Complaint Handling Process

Employees or the public may send PIPA-related questions and complaints to you or to the Office of the Information and Privacy Commissioner. Set up sound, specific practices to handle these inquiries, as well as requests for access to, or for correcting, personal information.

8. Review and Revise Forms, and Create Notice Statements

In most situations, when an organization collects personal information, the organization needs to give notice of the purposes for the collection. If an organization uses a service provider outside of Canada to collect or process personal information, the organization must also notify the individual of how to access the organization's policies on its use of service providers, as well as the position name of a person who is able to answer questions about the use of the service providers. Add these notices to forms and websites as necessary. Make sure the paper and online versions of the forms and notices are kept current and say the same thing.

9. Review and Revise Contracts

Your responsibility to protect personal information continues when the organization provides personal information to a contractor for processing. Contracts should contain clauses to clarify that the organization is legally responsible for that personal information. They should set out expectations regarding the collecting, using, and disclosing of personal information on the organization's behalf.

Your organization can develop standard wording for agreements with contractors when personal information is disclosed for processing.

10. Consider Employees' Personal Information

Personal employee information is also covered by the Act. "Personal employee information" is, in respect of an individual who is a potential, current or former employee of an organization, personal information reasonably required by the organization for the purposes of establishing, managing or terminating an employment or volunteer work relationship, or managing the post- employment or post-volunteer work relationship. While consent is not required to collect, use or disclose personal employee information, activities unrelated to managing employees may require consent. An organization will need to decide when it requires an employee's consent to collect, use, or disclose personal information. Build these processes into your normal business practices.

More Information

Office of the Information and Privacy Commissioner of Alberta

Phone: 780-422-6860
Toll free: 1-888-878-4044
Email: generalinfo@oipc.ab.ca
Website: www.oipc.ab.ca

Service Alberta – PIPA Help Desk

Phone: 780-427-5848
Toll free: 310-0000, then 780-427-5848
Email: sa.accessandprivacy@gov.ab.ca
Website: www.pipa.alberta.ca