PIP Home

Personal Information Protection

Private Sector Privacy Legislation

Implementation Tools

Table of Contents

PIPA Tools TOC

Personal Information Protection

Private Sector Privacy Legislation

PIPA Implementation Tool 1

Ten Steps To Compliance: What you can do now to prepare for January 1, 2004

Private Sector Privacy

On January 1, 2004, the *Personal Information Protection Act* (PIPA) comes into effect. PIPA will regulate the way private sector organizations collect, use, keep secure and disclose personal information.

PIPA will ensure that organizations that hold information about individuals handle that personal information responsibly. It also gives individuals control over the way information about them is handled and a right to request access to and correction of their personal information.

Organizations covered by PIPA need to consider how they will comply with and implement PIPA's privacy protection provisions. (For more information on whether your organization is covered refer to "How do I know if I am covered?").

The way an organization approaches compliance will vary depending on a number of factors, including:

- the nature of the organization's business;
- the organization's size;
- the kind of information the organization collects, uses and discloses;
- how the organization stores and secures information;
- the expectations of the individuals who deal with the organization;
- whether the organization transfers personal information across provincial or national borders; and,
- the reputation the organization wishes to promote.

Developing a Privacy Plan

Developing a Privacy Plan is a good place to start. While not an exhaustive list, a privacy plan usually includes the following ten steps:

1. Assign Responsibility

An organization must designate one or more individuals within the organization to be responsible for developing and implementing a privacy policy that suits the organization's business and complies with the law (this individual is commonly known as a "Privacy Officer").

The Privacy Officer is the first point of contact in the organization when privacy issues arise either internally or from outside the organization. The Privacy Officer is responsible for ensuring that the organization's privacy policy and procedures are fully implemented and working effectively.

Other activities could include:

- formulating, coordinating and implementing a privacy policy plan. This plan could include conducting or coordinating a privacy audit and undertaking risk assessment; and,
- promoting the plan to all relevant parties.

For more information on what a Privacy Officer does, refer to "What is a Privacy Officer?".

2. Become Familiar with the Ten Privacy Principles

The next step is for relevant members of the organization to familiarize themselves with PIPA's privacy principles. The ten privacy principles are legally binding rules that regulate the way private sector organizations collect, use, disclose, and ensure the security of personal information.

These principles (commonly know as "Fair Information Practices") are internationally recognized as fundamental to the protection of personal privacy and are found in most privacy legislation around the world. PIPA's privacy principles are the same as those set out in the Canadian Standards Association's Model Code for the Protection of Personal Information which was incorporated into the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA).

An organization will need to become familiar with the privacy principles in order to design and implement a compliant privacy program. For more information on these principles refer to the Ten Principles for the Protection of Privacy.

3. Conduct a Privacy Audit

In order to identify what you will need to do to comply with PIPA, it is critical to find out where you are now. The first question to ask is "Where do we have personal information and how do we currently manage it?"

A privacy audit will assist you in answering these two questions and prepare you for assessing how your current practices measure up against the Ten Principles for the Protection of Privacy.

A privacy audit is not a complicated process that involves hiring a professional auditor. It simply means conducting an internal inventory and review of your personal information holdings and practices.

A privacy audit involves the following three steps which may be performed together or in order: taking an inventory of your personal information holdings; identifying the information needs of the different functions within your organization; and identifying your current information practices (including how and why your

organization collects, uses and discloses personal information).

The amount of time and resources that need to be devoted to a privacy audit will depend on the size of your organization, the amount of personal information you hold, and the complexity of your information handling practices.

For more information, on how to conduct a privacy audit, refer to Conducting a Privacy Audit of your Personal Information Holdings.

4. Put your Practices to the Test

Having conducted a Privacy Audit of your organization's information handling practices, the next step is to assess how those practices measure up against the privacy principles found in PIPA, PIPEDA and other privacy legislation. A plan can then be developed to address any areas that do not comply with these principles.

The Privacy Compliance Self-Assessment Tool was developed to assist organizations to self-assess their readiness for privacy legislation. The tool assesses an organization's compliance with the Ten Principles for the Protection of Privacy through a series of questions and generates a report outlining the additional steps an organization should take to be fully compliant by January 1, 2004.

5. Implement Changes

After auditing and analysing your information handling practices, you may need to implement certain changes to your information practices and systems (technological and otherwise).

Staff who are responsible for developing your privacy plan are not necessarily those you will need to implement it. Regardless of the size of your company, ideally, any area that collects, uses or discloses personal information should be involved in the implementation of your privacy program. For example, implementing changes to how your organization collects, uses and discloses employee information should involve Human Resources personnel.

Few organizations conduct business or deliver services without employing some form of information technology. Compliance with the privacy principles may require a change to some of your information systems. For example, you may need to update your computer databases so you can retrieve the personal information of a specific individual when requested, or you may need to eliminate automatic or invisible collection of personal information on your Web site.

6. Develop a Privacy Policy

Good privacy practice often depends on the context in which personal information is handled and the expectations of the individuals interacting with an organization. Discussing privacy expectations with staff and customers/clients and thinking about ways to address their concerns will give an organization a sound basis for a privacy policy.

It may also be helpful to work with an industry association or other industry participants when developing a privacy policy. Organizations may find that their industry body has already thought about many of the privacy issues that arise in the industry.

7. Train Staff

The way an organization's staff handle personal information is just as important as the technology the organization has in place to manage and secure the information. A privacy plan should include a program to train staff about privacy procedures and the organization's privacy policy.

Your staff will need to understand that there will be legislative requirements placed on your organization in 2004 and that these requirements may necessitate changes in some of their jobs, tasks and responsibilities.

No matter how good your privacy policy and practices are on paper, or how secure your technology is, it is your staff who will be responsible for consistently complying with the privacy principles on a transaction-by-transaction basis. Therefore, staff training will be essential to your success in this area.

Every one of your employees, associates, contractors, partners, or agents who collect, use or disclose personal information will need to understand that they must do so in accordance with PIPA's privacy principles and your stated privacy policy.

The training needs of your staff (i.e., the type, scope, frequency and content) will vary according to the nature of their responsibilities. It is likely that you will need to undertake some sort of general education, as well as job-specific training for those new and existing staff responsible for managing personal information.

8. Develop or revise forms and communications materials

Review and revise as necessary your organizations forms, brochures, websites, etc. to comply with, and inform your customers or clients about your privacy policy and information practices. If your organization collects personal information by forms, or online, you will need to include notices that inform individuals of the collection purposes.

9. Review and revise service contracts

Your organization is responsible for personal information in its custody (i.e., physically held by) as well as information under its control (i.e., ownership, responsibility). This includes personal information that your organization has transferred to a contractor for processing or information the contractor may have collected on your organization's behalf.

To ensure that this personal information is properly protected, your contracts should clearly state what requirements must be met to comply with applicable privacy legislation and any policies your organization has developed to properly manage personal information.

For sample contract language, please see the Privacy Protection Schedule Template. Attaching this schedule or a similarly worded schedule to your agreements with third parties should enable your organization to comply with its privacy responsibilities.

10. Develop an effective complaints handling process

A privacy plan should include a process for handling privacy complaints. It is always more efficient for an organization to resolve complaints directly than to involve an outside regulator. Having an effective complaints handling process is an important part of managing privacy risks within an organization. It helps an organization to:

- address complaints quickly and effectively;
- identify (and address) any systemic or ongoing compliance problems;
- increase consumer confidence in the organization's privacy procedures;
- strengthen the good reputation of the organization; and,
- avoid an investigation by the Information and Privacy Commissioner.

For tips on how to set up an effective complaints process, see Setting Up a Complaint Handling Process.

PIPA Tools TOC

Personal Information Protection

Private Sector Privacy Legislation

PIPA Implementation Tool 2

"How Do I Know if I'm Covered?"

This purpose of this tool is to assist British Columbia private sector organizations in determining if the *Personal Information Protection Act* (PIPA) will apply to them.

It lists the type of private sector organizations that PIPA will apply to and those that will be exempt from its coverage. This guide also describes the types of information and information purposes that are exempt from coverage by PIPA and clarifies the relationship between PIPA and other provincial and federal privacy legislation.

Covered by PIPA

1. PIPA applies to **every** organization except where noted.

2(a) PIPA defines an "organization" as including

- a person (e.g., corporation, partnership)*;
- an unincorporated association body;
- a trade union;
- a trust; or,
- a not-for-profit organization.

* According to the *Interpretation Act,* "person" includes a corporation, partnership or party, and the personal or other legal representatives of a person to whom the context can apply according to law.

(b) It is important to note that the definition of "organization" is illustrative rather than exhaustive. For example, an entity may still be covered by PIPA even though it is not specifically included in the definition because, as noted below, it is not specifically excluded.

Not Covered by PIPA

3. PIPA further qualifies the term "organization" by stating that some entities are not organizations (and so are not covered by PIPA). The following entities are deemed not to be organizations for the purpose of PIPA:

- an individual acting in a personal or domestic capacity or acting as an employee,
- a public body as defined in the *Freedom of Information and Protection of Privacy Act*,

- the Provincial Court, the Supreme Court or Court of Appeal,
- the Nisga'a Government, as defined in the Nisga'a Final Agreement, or
- a private trust for the benefit of one or more designated individuals who are friends or members of the family of the settlor.

4. Certain types of personal information and certain collection, use or disclosure purposes are also exempt from PIPA's coverage. So even where an organization would otherwise be covered by PIPA, if the personal information falls under one of the excepted categories, that personal information is not covered by PIPA.

5. Further to items 3 and 4, PIPA **does not apply** to the following entities, personal information, and collection, use or disclosure purposes:

Personal or Domestic Purposes

While PIPA would apply to an individual who collects, uses or discloses personal information in a commercial capacity (i.e., home-based mail-order business, wedding videographer), it does not apply where an individual collects, uses or discloses personal information solely for personal or domestic purposes (i.e., Christmas card mailing list, home movies).

Individual acting as an employee

An organization is responsible for the personal information its employees (including volunteers) collect, use and disclose and the ways in which its employees handle personal information. PIPA applies to the organization - not the individual employee.

For example, PIPA would apply to a society raising funds to send children to camp. Any personal information collected by the society's employees and volunteers during the fundraising drive is collected on behalf of the society. It is the society, therefore, that is responsible for the methods the canvassers use to collect personal information and the manner in which the canvassers handle the personal information.

Journalistic, artistic or literary purposes

PIPA does not apply to the collection, use or disclosure of personal information solely for journalistic, artistic or literary purposes. This exemption reflects the *Charter* right to freedom of expression for newspapers.

PIPA does, however, still apply to the media to the extent that the media collects, uses or discloses personal information for other unrelated purposes, such as marketing. PIPA will also apply to the personal employee information of journalists

The *Freedom of Information and Protection of Privacy Act* applies

PIPA does not apply to a public body, as defined in Schedule 1 of the *Freedom of Information and Protection of Privacy Act* (FOIPP Act), or to the personal information in the custody or control of a public body. This is because these bodies, and the personal information in the custody or control of these bodies, are already covered by the FOIPP Act.

Some examples of public bodies are:

- a ministry of the government of British Columbia;
- a provincial agency, board, commission, corporation, etc. listed in Schedule 2 of the FOIPP Act;
- a municipality;

- a municipal police board;
- a hospital;
- a regional health authority;
- a university;
- a school board;
- health care body;
- a self-governing body of a profession or occupation (e.g., College of Physicians and Surgeons)

Contractors to public bodies

In addition to personal information held by public bodies, the FOIPP Act also applies to personal information that, while not in the custody of (i.e., physically held by) the public body, is under its control (i.e., ownership, responsibility).

For example, a third party organization, such as a data processor or an independent contractor, may receive personal information from a public body or collect personal information for a public body in the course of carrying out work on behalf of the public body under a contract. While the personal information may be in the custody of the third party organization, it remains under the control of the public body. Therefore, the FOIPP Act applies to this personal information and PIPA does not.

However, if a public body discloses personal information to a third party organization and **does not** retain control over the information, the collection, use and subsequent disclosure of the personal information by the organization is covered by PIPA.

The Personal Information Protection and Electronic Documents Act applies

The federal *Personal Information Protection and Electronic Documents Act* applies to federally-regulated organizations such as banks, telecommunications companies, airlines, railways and interprovincial trucking companies. It also applies to personal information that any organization discloses across borders for a commercial purpose (e.g., the sale or lease of client lists).

Even if the organization or personal information is located in British Columbia, if the federal *Personal Information Protection and Electronic Documents Act* applies to it (i.e., to the extent that the organization is federally-regulated or the personal information is disclosed across borders for a commercial purpose) then PIPA does not apply.

Court, Judicial and Quasi-Judicial Records

PIPA does not apply to the Provincial Court, the Supreme Court, the Court of Appeal or any court document.

PIPA does not apply to any document of a judge of the aforementioned courts (including those relating to support services provided to a judge), a master of the Supreme Court or a justice of the peace. It also does not apply to a judicial administration record which is a record containing information relating to a judge, master or a justice of the peace (e.g., a scheduling record of judges and trials).

PIPA similarly does not apply to a note, communication or draft decision of a decision maker in an administrative proceeding.

Prosecution documents

PIPA does not apply to documents related to a prosecution if all proceedings related to the prosecution have not been completed.

MLAs and Officers of the Legislature

PIPA does not apply to the collection, use or disclosure of personal information by a Member of the Legislative Assembly or an Officer of the Legislature (e.g., Auditor General, Ombudsman, Information and Privacy Commissioner, etc.) that relates to the exercise of the functions of that member or officer.

The Collection of Personal Information Collected on or before PIPA Comes into force

PIPA does not apply to the collection of personal information that was collected on or before it comes into force (i.e., before January 1, 2004).

It is important to note that it is only the collection process that is "grandfathered". What this means is that an organization that collected personal information before PIPA comes into force will not have to recollect that information under the new rules.

However, PIPA will still apply to how an organization uses, secures and discloses the personal information that was collected before it comes into force and individuals will have a right of access and a right to request correction of their personal information that was collected before PIPA comes into force.

In order to comply with PIPA, an organization will have to ensure that it only uses and discloses personal information that it collected before PIPA comes into force for purposes that a reasonable person would consider appropriate in the circumstances and that fulfill the purposes for which it was originally collected.

PIPA Tools TOC

Personal Information Protection

Private Sector Privacy Legislation

PIPA Implementation Tool 3

"What is a Privacy Officer?"

1. What is a Privacy Officer?

A Privacy Officer is a person within an organization whose job it is to:

- encourage compliance with the Ten Principles for the Protection of Privacy and other provisions of the *Personal Information Protection Act* (PIPA);
- respond to requests for access to and correction of personal information and general issues concerning personal information and,
- work with the Information and Privacy Commissioner during the investigation of a privacy complaint against the organization.

A Privacy Officer may also be responsible for managing the necessary changes to an organization's:

- information management practices, policies and procedures;
- staff training;
- customer relations;
- policies and procedures; and,
- inquiry and complaint processes.

2. Why have a Privacy Officer?

The *Personal Information Protection Act* (PIPA) says that an organization must designate one or more individuals to be responsible for ensuring the organization complies with the Act.

The name of the privacy officer should be publicized within the organization and staff should be encouraged to discuss privacy issues with that person. As well, PIPA requires that the position name or title and contact information of each individual designated to be responsible for compliance be made available to the public.

3. Will one privacy officer be enough?

This depends on a number of factors such as:

- the size of the organization,
- the structure of the organization (is it in one place only, or does it have a number of offices or branches?),

- the amount of personal information the organization holds, and the type of activity it is engaged in.

A large organization with a number of branch offices might find it desirable to designate a privacy officer in each location. However, a company (either big or small) that holds very little personal information might find that one privacy officer in the head office (or the only office) is enough. A designated privacy officer may delegate his or her duties to another individual. However, any delegation should be a formal written delegation.

4. Does this mean that organizations need to hire extra staff?

In most cases, extra staff should not be necessary. It should be possible for an existing staff member to take on the duties of a privacy officer.

However, where the main business or activity of the agency is connected with the collection and use of personal information, these duties may warrant a full-time position.

5. Who else should know about the Protection of Privacy Principles and the *Personal Information Protection Act* (PIPA)?

Everyone in the organization who handles personal information should have a general understanding of the protection of privacy principles and the objectives of the *Personal Information Protection Act* (PIPA). The Privacy Officer should be able to provide assistance when a more detailed knowledge of the organization's responsibilities is required.

6. What is the privacy officer's role if a complaint is made to the Information and Privacy Commissioner?

If an individual complains to the Information and Privacy Commissioner that an organization has violated his or her privacy, the Information and Privacy Commissioner or one of his staff may contact the Privacy Officer to discuss the complaint, and to see whether there is any means of settling the matter. The Privacy Officer should provide whatever assistance is necessary.

The Privacy Officer may be asked to provide background information or identify the people in the organization who can do so.

7. Do Privacy Officers need any special training?

Privacy Officers need to be familiar with the protection of privacy principles in the legislation and should be knowledgeable of their organization's personal information management practices. However, no special training is required.

It is important, however, to give your designated privacy official senior management support and the authority to intervene on privacy issues relating to any of your organization's operations.

PIPA Tools TOC

Personal Information Protection

Private Sector Privacy Legislation

PIPA Implementation Tool 4

Ten Principles for the Protection of Privacy

Principle 1 - Be accountable

To comply with this principle, an organization should:

- Ensure that it complies with the ten principles for the protection of privacy.
- In complying with the principles, consider 'what a reasonable person would consider appropriate in the circumstances'.
- Be responsible, by contractual or other means, for all personal information under its control, including personal information that is not in its custody. This includes personal information transferred to another organization for processing. (See Privacy Protection Schedule Template).
- Appoint an individual (or individuals) to be responsible for its compliance (see 'What is a Privacy Officer?') and communicate the name or title and contact information to staff and the public.
- Develop and implement policies and practices for the handling of personal information and make this information available to the public on request.
- Develop and implement a complaint process to handle complaints about its personal information practices and make this information available to the public on request.

Principle 2 - Identify the purpose

To comply with this principle, an organization should:

- Identify the purpose(s) for which personal information is needed and how it will be used and disclosed before or at the time personal information is collected.
- Ensure that the collection of personal information is necessary to fulfill the purpose(s) identified.

- Ensure that the purpose(s) is limited to what a reasonable person would consider appropriate in the circumstances.

- Inform the individual from whom the information is collected, either verbally or in writing, before or at the time of collection why the personal information is needed and how it will be used.

- On request by the individual, provide the name or title and contact information of a person within the organization who is able to answer questions about the collection of personal information.

- When using an individual's personal information that has already been collected for a new purpose not previously identified, inform the individual of the new purpose and obtain consent prior to its use.

Principle 3 - Obtain consent

To comply with this principle, an organization should:

- Obtain consent from the individual whose personal information is collected, used or disclosed.

- Obtain the individual's consent before or at the time of collection, as well as when a new use is identified.

- In determining what form of consent to use (e.g., written, verbal, implied, opt-in or opt-out), consider both the sensitivity of the personal information and what a reasonable person would expect and consider appropriate in the circumstances.

- When obtaining express consent, inform the individual of the purposes for the collection, use or disclosure of personal information in a manner that is clear and can be reasonably understood.

- Never obtain consent by deceptive means or by providing false or misleading information about how the personal information will be used or disclosed.

- Never make consent a condition for supplying a product or a service unless the collection, use or disclosure of the personal information is necessary to provide the product or service.

- Should an individual wish to withdraw consent, explain the likely consequences of withdrawing consent.

- Never prohibit an individual from withdrawing consent to the collection, use or disclosure of personal information unless it would frustrate the performance of a legal obligation.

Principle 4 - Limit collection

To comply with this principle, an organization should:

- Only collect personal information for purposes that a reasonable person would consider appropriate in the circumstances.

- Limit the amount and type of personal information collected to what is necessary to fulfill the identified purposes.

- Before or at the time of collection, comply with Principles 2 and 3 by informing the individual of the purposes for collection and obtaining consent.

- Collect personal information directly from the individual it is about unless the Act or the individual authorizes the collection of personal information from another source.

Principle 5 - Limit use, disclosure and retention

To comply with this principle, an organization should:

- Use or disclose personal information only for the purpose(s) for which it was collected, unless the individual consents to the new purpose, or the use or disclosure is otherwise authorized by the Act.

- Only use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.

- Keep personal information only as long as necessary to fulfill the purpose(s) for which it was collected.

- Keep personal information that is used to make a decision about an individual for at least one year after using it so the individual has a reasonable opportunity to obtain access to it.

- Destroy, erase or render anonymous personal information as soon as it is no longer serving the purpose for which it was collected and is no longer necessary for a legal or business purpose.

Principle 6 - Be accurate

To comply with this principle, an organization should:

- Minimize the possibility of using incorrect or incomplete information when making a decision that affects an individual or when disclosing an individual's information to another organization by making reasonable efforts to ensure that the personal information it collects is accurate and complete.

Principle 7 - Use appropriate safeguards

To comply with this principle, an organization should:

- Make reasonable security arrangements to protect personal information in its custody or under its control. Such arrangements should include physical measures, technical tools, and organizational controls where appropriate.

- Safeguard personal information from unauthorized access, collection, use, disclosure, copying, modification or disposal by both individuals outside the organization as well as within.

- Protect personal information regardless of the format in which it is held (e.g., paper, electronic, audio, video).

Principle 8 - Be open

To comply with this principle, an organization should:

- Make the following information available to customers, clients and employees on request:
    - brochures or other information that explain its personal information policies and practices;
    - name or title and contact information of the person who is accountable for its personal information policies and practices;
    - name or title and contact information of the person who can answer questions about its purposes for collecting personal information;
    - how an individual can gain access to his or her personal information and the name or title and contact information of the person to whom access requests should be sent; and,
    - the process for making a complaint about its personal information practices.

Principle 9 - Give individuals access

To comply with this principle, an organization should:

For Access to Personal Information requests

- Upon request, provide applicants with:
    - access to their personal information;
    - an explanation of how their personal information is or has been used; and,
    - a list of any individuals or organizations to whom their personal information has been disclosed.
- Provide a copy of the information requested or a response that includes reasons for not providing access, subject to the exceptions set out in the Act, within 30 business days unless an extension of time is permitted under the Act.

  If all or part of the requested information is refused, provide the applicant with a response that includes:
    - reasons and the provision of the Act on which the refusal is based;
    - the name or title and contact information of someone who can answer the applicant's questions about the refusal; and,

- information on how to request a review by the Information and Privacy Commissioner.

For Correction of Personal Information requests

- Upon request, correct personal information that the organization verifies is inaccurate or incomplete.
- If a correction is made, send a copy of the corrected personal information to each organization to which the incorrect or incomplete information was disclosed in the past year.
- If no correction is made in response to an individual's request, annotate the personal information in (i.e., make a note) to indicate that a correction was requested but not made.

Principle 10 - Provide recourse

To comply with this principle, an organization should:

- Develop and implement simple and easily accessible complaint handling procedures. (See Setting Up a Complaint Handling Process).
- Inform complainants of avenues of recourse. These include the organization's own complaint process and the Information and Privacy Commissioner.
- Investigate all complaints received.
- Take appropriate measures to correct information handling practices and policies.

PIPA Tools TOC

Personal Information Protection

Private Sector Privacy Legislation

PIPA Implementation Tool 5

Conducting a Privacy Audit of Your Personal Information Holdings

How to Conduct a Privacy Audit

In order for an organization to identify what it needs to do to comply with the Ten Principles for the Protection of Privacy, it is critical to determine the current state of its personal information holdings and related procedures. The organization needs to know what it has in the way of personal information, where it is stored and how it is currently managed.

A privacy audit involves the following three steps which may be performed together or in order: taking an inventory of your personal information holdings; identifying the information needs of the different functions within your organization; and identifying your current information practices (including how and why your organization collects, uses and discloses personal information).

A privacy audit should be an internal function. It is a self-assessment tool. There is no obligation to make the findings public. Therefore, it is important to stress to staff participating in this audit that it is not a test. Its purpose is not to embarrass them or to call people to task. What is needed at this stage in the development of the privacy program is an accurate and thorough inventory and analysis. There are no right answers. The sole purpose of the audit should be to collect information that can inform the planning and decision-making process regarding the future application of privacy legislation to the organization.

Taking an Inventory

Begin the audit by taking an inventory of the organization's existing records and information management policies and practices. The time and effort involved in this process will vary depending upon the complexity of the personal information holdings.

For example, the organization may collect personal information about the public, customers, partners, employees, contractors, shareholders, vendors, and many other types of individuals. For each function in the organization, you will need to determine if it collects, uses or discloses any personal information and, if so, how that information is managed and by whom.

When identifying the organization's personal information holdings, be sure to examine records in hardcopy, on computers and other electronic media, as well as any online resources (e.g., Web sites, chat rooms, news services, mailing lists, or

bulletin boards) it operates.

While not an exhaustive list, the following areas commonly collect, use and disclose personal information:

- customer service;
- complaints;
- human resources;
- finance/purchasing;
- information technology;
- security; and
- legal services.

Additionally, you should think of all the points where the organization collects personal information. Examples may include:

- point-of-purchase;
- customer service numbers;
- kiosks;
- contests;
- e-mail;
- surveys;
- video cameras;
- audio tapes;
- marketing lists;
- loyalty programs;
- delivery services;
- warranties;
- bankruptcies;
- returns;
- application forms;
- order forms;
- Web sites;
- bulletin boards;
- chat rooms;
- call centres; and
- technology enablers

The main benefit of this inventory is to enable you to determine the extent to which PIPA will apply to the organization's functions and the necessary scope of the privacy program you will need to develop. For example, if the organization only has personal information on its employees, the scope of the privacy program will be much more limited than an organization that also has personal information relating to customers or other types of individuals with whom it does business.

Follow Up the inventory by Identifying Information Needs and Practices

Once you have determined what personal information the organization has and where it is held, the next step is to fully understand how and why it collects, uses and discloses personal information. A necessary follow-up to the inventory is to identify the information needs of the different functions within the organization, along with its current information practices.

To do this, you will need to determine how and why all the types of personal information the organization has are necessary to a particular function and to the organization's operation. The reasons why personal information is collected, used and disclosed, along with who can see what, when, where, how and why, all need to be identified, documented and analyzed. This is an essential step if you want to know if the information management practices are compliant with the Ten Principles for the Protection of Privacy.

In order to audit the organization's information needs and practices, you could utilize questionnaires, in-depth interviews, group discussions, file and policy reviews, sampling, or other means of identifying information practices. Regardless of the methods, the review should be comprehensive and cover all of the organization's operations.

Audit questions could include:

1. How does the organization collect personal information? (Common ways in which organizations collect personal information include standard forms, customer surveys, loyalty programs, online interaction, video cameras.)

2. Why does the organization collect the personal information? Does the organization need it for a function or activity?

3. Are individuals made aware that the organization is collecting their personal information?

4. Does the organization inform individuals of the purpose for collecting their personal information?

5. Does the organization obtain consent from individuals before collecting or using their personal information? If so, what processes (verbal statements, paper or electronic notices) are used to obtain consent?

6. How does the organization use personal information? (e.g., for specific business functions, for activities that solicit new business?)

7. Does the organization disclose personal information to anyone outside the organization?

8. Does the organization make individuals aware of the intended uses and disclosures of their personal information? If so, how are individuals informed?

9. Is the personal information the organization holds accurate, complete and up-to-date?

10. How does the organization store personal information? (e.g., paper files, cabinets, databases, audio, video).

11. Where does the organization store personal information? (Organizations may keep personal information stored in a single cabinet or database or it may be spread across the organization in a number of sites.)

12. Who has access to the personal information held by the organization and who actually needs to have that access?

13. Does the organization have measures to protect the personal information it holds from unauthorised access, collection, use, disclosure, copying or modification from individuals both within and outside the organization?

14. Does the organization contract out any functions or activities involving personal information? Does the organization take any privacy measures to protect this information?

15. How long does the organization retain personal information?

16. How does the organization destroy or dispose of personal information?

PIPA Tools TOC

Personal Information Protection

Private Sector Privacy Legislation

PIPA Implementation Tool 6

Privacy Compliance Assessment Tool

Is the Organization Accountable for its Information Practices?

To find out if the organization is accountable for its information practices, answer the following questions:

1. Has the organization designated an individual (or individuals) to be responsible for its compliance with the *Personal Information Protection Act* (PIPA)?

☐ Yes ☐ No

2. Has the organization developed and implemented the necessary policies and practices to meet its obligations for the proper handling of personal information?

☐ Yes ☐ No

3. Does the organization use contracts and/or other means to ensure that contractors providing services on its behalf that involve the collection, use or processing of personal information provide privacy protection equal to or superior to its own?

☐ Yes ☐ No

4. Has the organization developed and implemented a complaint process to handle complaints about its personal information practices?

☐ Yes ☐ No

Does the Organization Identify Purposes?

To find out if the organization complies with the requirement to identify collection purposes, answer the following questions:

1. Does the organization identify the purpose(s) for which personal information is needed and how it will be used, taking into account both primary and secondary purposes (i.e., audit, marketing, etc.)?

☐ Yes ☐ No

2. Does the organization inform the individual, either verbally or in writing, of the purposes for collecting the personal information before or at the time that it collects personal information?

☐ Yes ☐ No

3. Before using personal information for a new purpose, not previously identified, does the organization inform the individual of the new purpose and obtain consent prior to its use?

☐ Yes ☐ No

Does the Organization Obtain Consent?

To find out if the organization complies with the requirement to obtain consent for the collection, use and disclosure of personal information, answer the following questions:

1. Does the organization obtain consent from the individual whose personal information is collected, used or disclosed?

☐ Yes ☐ No

2. Does the organization, when obtaining consent, inform the individual of the purposes for the collection, use or disclosure of personal information in a manner that is clear and can be reasonably understood?

☐ Yes ☐ No

3. Does the organization obtain the individual's consent before or at the time of collection, as well as when a new use is identified?

☐ Yes ☐ No

4. Does the organization obtain consent **without** using deceptive means or false or misleading information about how personal information will be used?

☐ Yes ☐ No

5. Does the organization ensure that consent is **not** a condition for supplying a product or a service unless the collection, use or disclosure of the personal information is necessary to provide the product or service?

☐ Yes ☐ No

6. Does the organization, in determining what form of consent to use (e.g., written, verbal, implied, opt-in or opt-out), consider both the sensitivity of the personal information and what a reasonable person would expect and consider appropriate in the circumstances?

☐ Yes ☐ No

7. Does the organization permit an individual to withdraw consent to the collection, use or disclosure of personal information unless it would frustrate the performance of a legal obligation?

☐ Yes ☐ No

8. Does the organization, upon receipt of a notice to withdraw consent, inform the individual of the likely consequences of withdrawing consent?

☐ Yes ☐ No

Does the Organization Limit its Collection of Personal Information?

To find out if the organization complies with the requirement to limit collection of personal information to that which is necessary and reasonable, answer the following questions:

1. Does the organization only collect personal information for purposes that a reasonable person would consider appropriate in the circumstances?

☐ Yes ☐ No

2. Does the organization limit the amount and type of personal information it collects to only that which is necessary to fulfill the purpose(s)?

☐ Yes ☐ No

3. Does the organization collect personal information directly from the individual it is about unless the Act authorizes the collection of personal information without consent from another source?

☐ Yes ☐ No

Does the Organization Limit Its Use, Disclosure and Retention of Personal Information?

To find out if the organization complies with the requirement to limit its use, disclosure and retention of personal information to that which is necessary to fulfill identified purpose(s), answer the following questions:

1. Does the organization use or disclose personal information only for purposes that a reasonable person would consider appropriate in the circumstances?

☐ Yes ☐ No

2. Does the organization use or disclose personal information only for the purpose(s) for which it collected it, unless the individual consents to a new purpose, or the use or disclosure is otherwise authorized by the Act?

☐ Yes ☐ No

3. Does the organization retain personal information only as long as necessary to fulfill the purpose(s) for which it was collected or a related business or legal purpose?

☐ Yes ☐ No

4. Does the organization retain personal information that is used to make a decision about an individual for at least one year after using it so the individual has a reasonable opportunity to obtain access to it?

☐ Yes ☐ No

5. Does the organization destroy, erase or render anonymous personal information as soon as it is no longer serving the purpose for which it was collected and is no longer necessary for a legal or business purpose?

☐ Yes ☐ No

Does the Organization Ensure that Personal Information is Accurate and Complete?

To find out if the organization complies with the requirement to ensure that personal information is accurate and complete, answer the following questions:

1. Does the organization make reasonable efforts to ensure that the personal information it collects about an individual is accurate and complete if it is likely to be **used to make a decision** that affects the individual?

☐ Yes ☐ No

2. Does the organization make reasonable efforts to ensure that the personal information it collects about an individual is accurate and complete if it is likely to **disclose** the personal information to another organization?

☐ Yes ☐ No

Does the Organization Secure Personal Information?

To find out if the organization complies with the requirement to protect personal information by making reasonable security arrangements, answer the following questions:

1. Does the organization make reasonable security arrangements (including physical measures, technical tools, and organizational controls where appropriate) to protect personal information in its custody or under its control?

☐ Yes ☐ No

2. Does the organization, in determining what level of security arrangements are reasonable, take into account the sensitivity of the personal information in its custody or under its control?

☐ Yes ☐ No

3. Does the organization implement safeguards that protect personal information from unauthorized access, collection, use, disclosure, copying, modification or disposal by individuals both outside the organization as well as within?

☐ Yes ☐ No

4. Does the organization have in place security measures that protect personal information regardless of the format in which it is held (e.g., paper, electronic, audio, video).

☐ Yes ☐ No

5. Does the organization dispose of or destroy personal information in a way that prevents unauthorized parties from gaining access to it?

☐ Yes ☐ No

Is the Organization Open about its Information Practices?

To find out if the organization complies with the requirement to be open about its personal information practices, answer the following questions:

1. Does the organization make the following information available to customers, clients and employees on request?

(a) brochures or other information that explain its personal information policies and practices?

☐ Yes ☐ No

(b) name or title and contact information of the person who is accountable for its personal information policies and practices?

☐ Yes ☐ No

(c) name or title and contact information of the person who can answer questions about its purposes for collecting personal information?

☐ Yes ☐ No

(d) how an individual can gain access to his or her personal information and the name or title and contact information of the person to whom access requests should be sent?

☐ Yes ☐ No

(e) the process for making a complaint about its personal information practices (e.g., the process for making internal complaints as well as complaints to the Information and Privacy Commissioner)?

☐ Yes ☐ No

Does the Organization Allow Individuals Access to Their Personal Information and a Right to Request Corrections?

To find out if the organization complies with the requirement to permit individuals access to, and a right to request correction of, their personal information, answer the following questions:

For Access to Personal Information requests

1. Does the organization, upon request, provide applicants with:

(a) access to their personal information, subject to limited exceptions?

☐ Yes ☐ No

(b) an explanation of how their personal information is or has been used?

☐ Yes ☐ No

(c) a list of any individuals or organizations to whom their personal information has been disclosed?

☐ Yes ☐ No

2. Does the organization provide a copy of the information requested or a response that includes reasons for not providing access:

(a) within 30 business days unless an extension of time is permitted under the Act?

☐ Yes ☐ No

(b) for minimal or no cost?

☐ Yes ☐ No

3. Does the organization, if all or part of the requested information is refused, provide the applicant with a response that includes:

(a) reasons and the provision(s) of the Act on which the refusal is based?

☐ Yes ☐ No

(b) the name or title and contact information of someone who can answer the applicant's questions about the refusal?

☐ Yes ☐ No

(c) information on how to request a review by the Information and Privacy Commissioner?

☐ Yes ☐ No

For Correction of Personal Information requests

1. Does the organization, upon request, correct personal information that is found to be inaccurate or incomplete?

☐ Yes ☐ No

2. Does the organization, if a correction is made, send a copy of the corrected personal information to each organization to which the incorrect or incomplete information was disclosed in the past year?

☐ Yes ☐ No

3. Does the organization, if no correction is made in response to an individual's request, annotate the personal information in dispute (i.e., make a note) to indicate that a correction was requested but not made?

☐ Yes ☐ No

Does the Organization Have a Process for Handling Complaints?

To find out if the organization complies with the requirement to have a process it place for responding to complaints about the organization's personal information practices, answer the following questions:

1. Does the organization have a process in place for receiving and responding to complaints or inquiries about its personal information practices?

☐ Yes ☐ No

2. Does the organization investigate all complaints?

☐ Yes ☐ No

3. Does the organization, where a complaint is justified, take appropriate measures to rectify the situation including correcting information handling practices and policies where necessary?

☐ Yes ☐ No

Reset Form

Privacy comments or questions? E-mail us at CPIAADMIN@gems5.gov.bc.ca Last update October 30, 2003

Tools TOC

Personal Information Protection

Private Sector Privacy Legislation

PIPA Implementation Tool 7

Setting Up a Complaint Handling Process

The *Personal Information Protection Act* (PIPA) requires organizations to have a process in place that individuals can use to make complaints about the organization's compliance with the Act. As well, PIPA permits the Information and Privacy Commissioner to refer an individual's complaint against an organization back to the organization if he is not satisfied that the individual attempted to first resolve the complaint with the organization.

Having an accessible and effective complaint handling process is an important part of managing privacy risks within your organization because it helps you to:

- address complaints in a timely manner
- identify and address systemic or ongoing compliance problems;
- increase consumer confidence in your privacy procedures; and,
- demonstrate your commitment to privacy and build a good reputation for your organization.

REMEMBER...

The more accessible and responsive your organization's complaint-handling process is, the more effectively you can contain a potentially explosive situation and better preserve or restore customer or client confidence in your organization.

Setting up an Accessible and Responsive Complaint-Handling Process

1. Decide who in your organization will be responsible for receiving and handling complaints about the organization's compliance with the Act.
Although different individuals within the organization may be called upon to help investigate complaints, it is a good idea to have one department or individual responsible for receiving all complaints to ensure that they are responded to in a timely way. It is probably simplest for both customers and staff if the individual that is responsible for ensuring the organization complies with the Act (e.g., the Privacy Officer) is the same individual responsible for receiving and responding to complaints.

2. Develop and implement a complaint procedure that is easily accessible, understandable and simple to use.

3. The procedure on handling and responding to privacy complaints should be written and communicated to both staff (so they know what to do if they receive a complaint) and customers (so they know what to expect if they make a complaint). Such a procedure should address the following points.

4. Decide in what format you will accept complaints (e.g., verbal, in writing, by email). If you deal mainly with your customers in writing, you may wish to only accept complaints in writing. On the other hand, if most of your interactions with your customers are verbal, you may also wish to accept verbal complaints. Whatever you decide, your procedure should be adaptable where appropriate (i.e., it may not be reasonable to expect someone who cannot write - due to language or other difficulties - to make a complaint in writing).

FOR CONVENIENCE...

You may wish to develop a complaint form (or adapt an existing form) to assist complainants in documenting their complaint. This approach may also make it easier for your organization to collect the information you need to investigate and respond to the complaint.

5. When a privacy complaint is received by the organization, it should immediately be forwarded to the individual or department responsible for responding to privacy complaints (e.g., the Privacy Officer).

6. Staff, upon request, should be able to inform an individual of the procedure for making a complaint and who to contact within the organization about the complaint. A complainant should also be informed of the right to complain to the Information and Privacy Commissioner if he or she is not satisfied with the organization's response to the complaint.

7. When the complaint is received by the Privacy Officer (or other individual responsible for responding to privacy complaints), the date the complaint was received should be recorded.

8. If the complaint was received verbally, the nature of the complaint (e.g. delays in responding to a request, incomplete or inaccurate responses, or improper collection, use, disclosure or retention) should be recorded.

9. Acknowledge receipt of the complaint promptly (see template for *Acknowledging Receipt of a Complaint*).

10. Contact the individual to clarify the complaint, if necessary.

11. Investigate all complaints received. (For tips on how to conduct a privacy investigation, see Conducting a Privacy Complaint Investigation.)

12. Ensure your complaint process is fair, impartial and confidential.

TO BE FAIR...

The investigation of a complaint should be assigned to a person with the skills necessary to conduct it fairly and impartially. Only in extenuating circumstances (e.g., sole proprietorship) should the complaint be assigned to a person who is the subject of the individual's complaint.

13. Give the investigator access to all relevant records, employees or others who handled the personal information or access request.

14. Where the complaint is justified, take appropriate measures to rectify the situation, including correcting information handling practices and policies where necessary and communicating those changes to relevant staff.

15. Notify individuals of the outcome of investigations clearly and promptly, informing them of any relevant steps taken.

16. Record all decisions to ensure consistency in applying the Act.

17. Follow up to verify that required changes to policies, procedures or practices have been undertaken.

PIPA Tools TOC

Personal Information Protection

Private Sector Privacy Legislation

PIPA Implementation Tool 8

"Currently Under Development"

PIPA Tools TOC

Personal Information Protection

Private Sector Privacy Legislation

PIPA Implementation Tool 9

Model Contract Language (Privacy Protection Schedule)

See next page

PRIVACY PROTECTION SCHEDULE

This Schedule forms part of the agreement between

_____ (the "Organization") and

_____ (the "Contractor") respecting

_____ (the "Agreement")

Purpose

1. The purpose of this Schedule is to enable the Organization to comply with its statutory obligations under the *Personal Information Protection Act* with respect to "personal information", as defined in section 2 of this Schedule.

Definition of personal information

2. In this Schedule, "personal information" means information about an identifiable individual collected or created by the Contractor as a result of the Agreement or any previous agreement between the Organization and the Contractor dealing with the same subject matter as the Agreement.

Collection of personal information

3. Unless the Agreement otherwise specifies or the Organization otherwise directs in writing, the Contractor may only collect or create personal information that is necessary for the performance of the Contractor's obligations, or the exercise of the Contractor's rights, under the Agreement.

4. Unless the Agreement otherwise specifies or the Organization otherwise directs in writing, the Contractor must collect personal information directly from the individual the information is about.

5. Unless the Agreement otherwise specifies or the Organization otherwise directs in writing, the Contractor must tell an individual from whom the Contractor collects personal information:

   (a) the purpose for collecting it; and

   (b) on request by the individual, the position name or title and the contact information of the person designated by the Organization to answer questions about the Contractor's collection of personal information.

Consent for the collection, use or disclosure of personal information

6. Unless the Agreement otherwise specifies or the Organization otherwise directs in writing, the Contractor must not collect, use or disclose personal information about an individual without the consent of the individual to whom the information relates.

Withdrawal of consent

7. If an individual provides reasonable notice to the Contractor that the individual withdraws consent to the collection, use or disclosure of the individual's personal information, the Contractor must inform the individual of the likely consequences to the individual, if any, of withdrawing consent.

8. The Contractor must not prohibit an individual from withdrawing consent to the collection, use or disclosure of the individual's personal information, unless the withdrawal of consent would frustrate the performance of a legal obligation.

9. If an individual withdraws consent to the collection, use or disclosure of the individual's personal information, the Contractor must stop the collection, use or disclosure of the individual's personal information (unless it is permitted under the Act without consent).

Accuracy of personal information

10. The Contractor must make every reasonable effort to ensure the accuracy and completeness of any personal information it collects that is likely to be used by the Contractor or the Organization to make a decision that directly affects the individual the information is about or to be disclosed to another party.

Access to personal information

11. If the Contractor receives a request for access to personal information from a person other than the Organization, the Contractor must promptly advise the person to make the request to the Organization, unless the Agreement expressly requires the Contractor to provide such access, and provide the name or title and contact information of an official of the Organization to whom such requests are to be made.

Correction of personal information

12. Within 5 business days of receiving a written direction from the Organization to correct or annotate any personal information, the Contractor must annotate or correct the information in accordance with the direction.

13. When issuing a written direction under section 12, the Organization must advise the Contractor of the date the correction request was received by the Organization in order that the Contractor may comply with section 14.

14. Within 5 business days of correcting or annotating any personal information under section 12, the Contractor must provide the corrected information to any party to whom, within one year prior to the date the correction request was made to the Organization, the Contractor disclosed the information being corrected.

15. If the Contractor receives a request for correction of personal information from a person other than the Organization, the Contractor must promptly advise the person to make the request to the Organization unless the Agreement expressly requires the Contractor to make the correction or annotation and provide the name or title and contact information of an official of the Organization to whom such requests are to be made.

Protection of personal information

16. The Contractor must protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure, copying, modification or disposal.

Retention of personal information

17. Unless the Agreement otherwise specifies, the Contractor must retain personal information until directed by the Organization in writing to dispose of it or deliver it as specified in the direction.

Use of personal information

18. Unless the Organization otherwise directs in writing, the Contractor may only use personal information for the performance of the Contractor's obligations, or the exercise of the Contractor's rights, under the Agreement.

Disclosure of personal information

19. Unless the Organization otherwise directs in writing, the Contractor may only disclose personal information to any person other than the Organization if the disclosure is for the performance of the Contractor's obligations, or the exercise of the Contractor's rights, under the Agreement.

Inspection of personal information

20. In addition to any other rights of inspection the Organization may have under the Agreement or under statute, the Organization may, at any reasonable time and on reasonable notice to the Contractor, enter on the Contractor's premises to inspect any personal information in the possession of the Contractor or any of the Contractor's information management policies or practices relevant to its management of personal information or its compliance with this Schedule and the Contractor must permit, and provide reasonable assistance to, any such inspection.

Compliance with directions

21. The Contractor must comply with any direction given by the Organization under this Schedule

Notice of non-compliance

22. If for any reason the Contractor does not comply, or anticipates that it will be unable to comply, with a provision in this Schedule in any respect, the Contractor must promptly notify the Organization of the particulars of the non-compliance or anticipated non-compliance and what steps it proposes to take to address, or prevent recurrence of, the non-compliance or anticipated non-compliance.

Termination of Agreement

23. In addition to any other rights of termination which the Organization may have under the Agreement or otherwise at law, the Organization may, subject to any provisions in the Agreement establishing mandatory cure periods for defaults by the Contractor, terminate the Agreement by giving written notice of such termination to the Contractor, upon any failure of the Contractor to comply with this Schedule in a material respect

Interpretation

24. In this Schedule, references to sections by number are to sections of this Schedule unless otherwise specified in this Schedule.

25. Any reference to the "Contractor" in this Schedule includes any subcontractor or agent retained by the Contractor to perform obligations under the Agreement and the Contractor must ensure that any such subcontractors and agents comply with this Schedule.

26. The obligations of the Contractor in this Schedule will survive the termination of the Agreement.