II.A.1 Ten Principles of Privacy Protection

Sometimes called “Fair Information Practices," the ten principles of privacy protection are internationally recognized and are found in most privacy legislation around the world. These principles inform the way private organizations collect, secure, use and disclose personal information.

Your organization must become familiar with the ten principles of privacy protection in order to develop, implement and maintain an appropriate privacy program.

The ten principles of privacy protection are:

1. Be accountable
2. Identify the purpose
3. Obtain consent
4. Limit collection
5. Limit use, disclosure and retention
6. Be accurate
7. Use appropriate safeguards
8. Be open
9. Give individuals access
10. Provide recourse

Be Accountable

To comply with this principle, you must:

- Be responsible, by contractual or other means, for all personal information under your control. This includes personal information shared with or transferred to another organization
- Designate a privacy officer and communicate the title and contact information to staff and the public
- Develop and implement policies and practices for handling personal information and make this information available to the public on request
- Develop and implement a process to handle complaints about your personal information practices and make this information available to the public on request
- Consider what a reasonable person would deem appropriate whenever you make privacy decisions
- Ensure your organization complies with all ten principles of privacy protection

Identify the Purpose

To comply with this principle, you must:

- Before or at the time of collection, identify the purpose for collecting personal information, including how it will be used
- Ensure the collection of personal information is necessary to fulfill the purpose identified
- Ensure the purpose is limited to what a reasonable person would deem appropriate
- Inform the individual from whom the information is collected, either verbally or in writing and before or at the time of collection, why their personal information is required and how it will be used
- Provide the title and contact information of your privacy officer, on request
- When using personal information for a new purpose not previously identified, inform the individual of the new purpose and obtain consent prior to its use

Obtain Consent

To comply with this principle, you must:

- 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 and when a new use is identified
- When determining what form of consent to use, such as written, verbal, implied, opt-in or opt-out consent, consider both the sensitivity of the personal information and what a reasonable person would deem appropriate
- When obtaining consent, clearly and transparently inform the individual of the purpose for the collection, use or disclosure of personal information
- Never obtain consent by deceptive means or by providing false or misleading information
- 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
- If an individual chooses 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 withdrawing consent would conflict with a legal obligation

Limit Collection

To comply with this principle, you must:

- Before or at the time of collection, inform the individual of the purposes for collecting personal information
- Only collect personal information for a purpose that a reasonable person would deem appropriate
- Limit the amount and type of personal information collected to what is necessary to fulfill the purpose identified before or when it was collected
- Collect personal information directly from the individual unless the legislation or the individual authorizes the collection of personal information from another source

Limit Use, Disclosure and Retention

To comply with this principle, you must:

- Use or disclose personal information only for the purpose identified before or when it was collected, unless the individual consents to the new purpose, or the use or disclosure is authorized by the legislation
- Only use or disclose personal information for purposes that a reasonable person would deem appropriate
- Keep personal information only as long as necessary to fulfill the purpose identified before or when 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 access it
- Destroy, erase or make anonymous any personal information as soon as it is no longer required for a legal or business purpose

Be Accurate

To comply with this principle, you must:

- Make reasonable efforts to ensure that the personal information you collect is accurate and complete
- 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

Use Appropriate Safeguards

To comply with this principle, you must:

- Make reasonable security arrangements to protect personal information under your control, including physical measures, technical tools and organizational controls where appropriate
- Safeguard personal information from unauthorized access, collection, use, disclosure, copying, modification or disposal by individuals from within and outside your organization
- Protect all personal information regardless of its format, including paper, electronic, audio, and video data.

Be Open

To comply with this principle, you must make the following information available to customers, clients and employees on request:

- The title and contact information of your privacy officer in order to explain personal information policies and practices or answer questions about the purpose for collecting personal information
- The process an individual can follow to gain access to his or her personal information and the title and contact information of the employee an individual can contact to make such a request
- Information that explains your organization's personal information policies and practices
- The process for making a complaint about your organization's personal information practices

Give Individuals Access

Requests for access to personal information fall into three categories:

- Access requests that are allowed
- Access requests that are refused
- Access requests to correct personal information

Access requests that are allowed

If all or part of the access request is allowed, you must provide the individual with:

- Access to their personal information in the form of a copy of the information requested, within 30 business days (unless an extension of time is permitted in the legislation)
- An explanation of how their personal information is or has been used
- A list of any individuals or organizations to whom their personal information has been disclosed

Access requests that are refused

If all or part of the access request is refused, you must provide the applicant with:

- A response that includes the legal reason(s) for the refusal, within 30 business days
- The title and contact information of your privacy officer should the applicant have questions about the refusal
- Information on how to request a review by the Information and Privacy Commissioner

Access requests to correct personal information

For access requests to correct personal information, you must:

- Correct any personal information discovered to be 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, annotate the personal information to indicate that a correction was requested but not made

Provide Recourse

To comply with this principle, you must:

- Develop and implement simple and accessible complaint handling procedures
- Investigate all complaints received
- Take appropriate measures to correct your information handling practices and policies
- Inform complainants of their avenues of recourse, including your organization's own complaint process and the Information and Privacy Commissioner's complaint process

Information & Privacy Commissioner

The Office of the Information and Privacy Commissioner offers a number of tools and resources for private organizations.

Legislation

- *Personal Information Protection Act*

Contact Information

Office: 250 356-1851

Email: privacy.helpline@gov.bc.ca