The Personal Information Protection and Electronic Documents Act: A Guide for Insurance Brokers

This guide has been written by Steven C. Gaon, Barrister & Solicitor, on behalf of the Insurance Brokers Association of Canada.

Disclaimer: This guide is presented for general legal information only. It is not intended to provide specific legal advice and accordingly, should not be relied upon as a binding opinion on the matters addressed within. While great care was taken to ensure the accuracy of the guide's contents, you should seek and be guided by legal advice based on your specific circumstances.

TABLE OF CONTENTS

I Introduction

When does the Act apply?

- The Personal Information Protection and Electronic Documents Act ("the Act") came into force on January 1, 2001. It immediately applied to all "federal works, undertakings and businesses".

- **Insurance brokers operating strictly within a province are not required to comply with the Act until January 1, 2004. *However* if** a broker organization collects, uses or discloses personal information in connection with the operation of a federal work, undertaking or business or **a broker discloses personal information *outside* the province for consideration, the broker must comply with the Act immediately.**

About the Act

The stated purpose of the Act is to recognize the privacy rights of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for reasonable purposes. This is unusual legislation in that it not only contains mandatory language ("shall") and permissive language ("may"), it also uses the word "should", which, according to the Act, indicates a recommendation and not an obligation. Although this Guide will focus mainly on the obligatory provisions, insurance brokers will be encouraged to follow the various recommendations as well.

About this Guide

This Guide is divided into logical sections that generally correspond to the Act and to Schedule 1 of the Act. The author has already cross-referenced where appropriate, so it will not be necessary for the reader to go back and forth, for example, between the Act and Schedule 1. The Guide also provides illustrative examples throughout to give practical examples and tips on how to comply with the Act. At the end of the Guide is a Privacy Questionnaire that may be used along with description of the Act and the illustrative examples. Answering “no” to questions indicates areas that need to be addressed or improved.

What Remedies and Sanctions are Available under the Act?

- An individual may complain to your organization about an alleged violation of the Act or may file a written complaint with the Privacy Commissioner of Canada.

- The Commissioner may also initiate a complaint and conduct an investigation in respect of any complaint. The Commissioner has wide powers to investigate, conduct an audit and gather evidence. If the Commissioner finds the allegations to be supported by the evidence, a report will be issued to the parties. Once that happens, either the individual complainant or the Commissioner may apply to the Federal Court. The Court may order an organization to correct its practices, order an organization to publish a notice of any action taken or proposed to correct its practices, and award damages to the complainant, including damages for the humiliation a complainant has suffered.

- The Act also contains a number of **sanctions**. Every person who knowingly:

  - fails to retain personal information long enough for individuals to exhaust any recourse they may have under this Act;
  - takes any action against an employee who has complained to the Commissioner about your organization or who refuses to do something that is in contravention of the Act; or
  - obstructs the Commissioner in the investigation or in the audit;

  is guilty of:

  (a) an offence punishable on summary conviction and liable to a fine not exceeding $10,000; or
  (b) an indictable offence and liable to a fine not exceeding $100,000.

II Key Definitions

- "Commissioner" means the Privacy Commissioner of Canada.

- "consent" – consent may be express (written or oral) or implied by the circumstances.

- "federal work, undertaking or business" means any work, undertaking or business that is within the legislative authority of Parliament (such as transportation, telecommunications, broadcasting, banking, etc.).

- "organization" includes an association, a partnership, a person and a trade union.

- "personal information" means information about an identifiable individual, but does not include an employee's name, title, business address or telephone number.

III Basic Obligations

The Act creates obligations and restrictions regarding the *collection*, *use* and *disclosure* of personal information. Organizations may only collect, use or disclose the personal information of others for purposes that a "reasonable person would consider appropriate". This is an objective standard, which means you should govern how you handle a client's personal information not by what *you* think is appropriate but by what a *client* or the *general public* is likely to consider appropriate.

IV The Ten Principles

The Act contains a schedule (Schedule 1) enunciating 10 guiding principles and numerous related rules. These principles are set out and explained in the pages that follow.

Note: All of the dark triangular bullet points which follow are taken directly from the Act and should be adhered to as strictly as possible.

1. Accountability

- Every organization must designate at least one individual who is accountable for that organization's compliance with the Act. The designated individual's name must be made known upon request. This duty can be delegated but accountability still lies with that person.

  Illustrative Example: *D*esignate a senior person to be the "privacy officer". Tell the receptionist who that person is so clients can easily be informed.

- Organizations are responsible for personal information that has been *transferred* to a third party for processing. The organization must use contractual or other means to provide a comparable level of protection while the information is being processed by a third party.

  ***Illustrative Example*:** If you are sending a client's personal information to an insurance company or other third party, you should obtain a written confirmation that the third party will comply with the Act. Transmission to a third party includes contracting out services such as adjusting or legal work. Ask for the name of the third party's privacy officer and for a copy of that organization's written policies on the protection of personal information. Ensure that those policies provide a comparable level of protection and where possible, obtain such assurances in writing. If not practical to obtain a written assurance, make a written notation in your own file.

- Organizations must implement written policies and practices to give effect to the 10 principles, including the implementation of procedures to:

  (a) protect personal information,
  (b) allow individuals to file complaints against your organization,
  (c) train and educate staff, and
  (d) develop information which explains those procedures to the public.

  Illustrative Example: As set out in Principle 8 "Openness", an organization may choose explain its policies and practices to the public by:

  - making brochures available in its place of business;
  - mailing information to customers;
  - providing website access;
  - establishing a toll-free telephone number.

  Each of the above methods of public accessibility should include the privacy officer's *name* and *telephone number*, as well as *information on how someone may amend any inaccuracy* in their personal information. Individuals should also be informed on *how to file a complaint* about your organization's use or disclosure of personal information.

2. Identifying Purposes

- The purposes for which personal information is collected must be clearly identified by the organization at or before the time the information is collected. Depending upon the way in which the information is collected, this can be done orally or in writing. An application form, for example, may give notice of the purposes.

  Illustrative Example: The organization should have a form for clients to sign which explains the purposes for which specific information is needed. This will accomplish two goals: it will explain the purposes for collection *and* it will secure the required consent for collection (see also Principle 3 "Consent" and Principle 4 "Limiting Collection").

- The organization must document the purpose(s) for which personal information is collected. Organizations collecting, using or disclosing personal information for a new purpose must document this new purpose.

  Illustrative Example: This can be done by way of a typed note in your client file.

- When personal information that has been collected is to be used for a purpose not previously identified, the new purpose must be identified prior to use. Generally you must obtain the express consent of the individual before information can be used for that new purpose.

  Illustrative Example: If you intend to give a client's personal information to another organization for the purpose of cross-marketing, that is a "new purpose"; you must identify that new purpose in writing and obtain prior consent (preferably in writing).

3. Consent

- Consent of the individual is required for the collection of personal information and the subsequent use or disclosure of this information, subject only to the exceptions which are set out in section V of this Guide.

  Illustrative Example: Before you collect information from an up-to-date "driver's abstract", you should obtain the consent of the insured person. Consent is not needed from an individual under investigation for insurance fraud.

- The form of the consent may vary. **Express** consent can be given *orally* or in *writing*. Consent may be also be **implied** by the circumstances.

- In obtaining consent, the reasonable expectations of the individual are relevant.

  Illustrative Examples:

  - Express *written* consent would include a client signing a consent form or providing you with a letter specifically authorizing you to obtain certain information.

  - Express *oral* consent can be given over the telephone.

  - Implied consent is one in which you have not received a specific authorization but the circumstances allow you to obtain, use or disclose the information.

  - ***However*, you should generally try to seek the 'highest' form of consent, which is to say *express*, *written* consent.** If you cannot obtain signed consent, at a minimum, document the client's approval by way of a memo in the file.

  - If you are simply renewing an insurance policy at a client's request, it is reasonable to assume that there is an implied consent to use the existing client information. However, if you plan to send this information to a new insurance company, you need an express consent to do so.

- Individuals can give express consent in many ways. For example:

  (a) an application form may be used,
  (b) a check-off box may be used – individuals who do not check the box are assumed to consent to the transfer of information to third parties,
  (c) consent may be given orally when information is collected over the telephone, or
  (d) consent may be given at the time that individuals use a product or service.

- An organization may not, as a condition of the supply of a product or service, require an individual to consent to the collection, use, or disclosure of information beyond that required to fulfil explicitly specified and legitimate purposes.

  Illustrative Example: It is not acceptable to make a client to sign an overly broad, blanket authorization at the outset of the business relationship.

- An individual may withdraw consent at any time and the organization must inform the individual of the implications of such withdrawal.

4. Limiting Collection

- The collection of personal information must be limited to that which is necessary for the purposes identified by the organization. Personal information cannot be collected indiscriminately.

- Information must be collected by fair and lawful means and not by misleading or deceiving individuals about the purpose for which information is being collected.

5. Limiting Use, Disclosure and Retention

- Personal information cannot be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law.

  Illustrative Example: It is not acceptable to use personal information acquired to provide a P&C insurance policy to cross-sell your business' other services without the consent of the individual.

- Personal information must be retained only as long as necessary for the fulfillment of those purposes.

- Organizations should develop guidelines and implement procedures with respect to the retention of personal information which should include minimum and maximum retention periods. Personal information that has been used to make a decision about an individual must be retained long enough to allow the individual access to the information after the decision has been made.

- Personal information that is no longer required to fulfil the identified purposes should be destroyed, erased, or made anonymous. Organizations must develop guidelines and implement procedures to govern the destruction of personal information.

6. Accuracy

- Personal information – including information that is disclosed to third parties – must be as accurate, complete and up-to-date as is necessary for the purposes for which it is to be used.

- Organizations must minimize the possibility that inappropriate information may be used to make a decision about an individual.

- Organizations must not routinely update personal information, unless such a process is necessary to fulfil the purposes for which the information was collected.

  Illustrative Example: In an insurance broker's field of work, it is reasonable to assume that a regular updating process is generally necessary and appropriate.

7. Safeguards

- Personal information must be protected by security safeguards appropriate to the sensitivity of the information.

- The security safeguards must protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification. Organizations must protect personal information regardless of the format in which it is held.

- The nature of the safeguards will vary depending on the sensitivity of the information that has been collected, the amount, distribution, and format of the information and the method of storage. More sensitive information should be safeguarded by a higher level of protection.

  Illustrative Example: Assume all client personal information is sensitive and seek to achieve the highest level of security. When transferring client information to a third party, remove or mask any information that is not strictly needed by the third party.

- The methods of protection should include:

  (a) physical measures, such as locked filing cabinets and restricted access;
  (b) organizational measures, such as security clearances and limiting access on a "need-to-know" basis; and
  (c) technological measures, such as the use of passwords and encryption.

- Organizations must make their employees aware of the importance of maintaining the confidentiality of personal information.

  Illustrative Example: Consider having monthly or quarterly staff meetings on the subject. Ensure that your policies are clearly communicated and accessible to all employees. Review policies regularly and revise where appropriate.

- Care must be used in the disposal or destruction of personal information to prevent unauthorized parties from gaining access to the information.

  Illustrative Example: When disposing of client documents, do not put them in a recycle box (unless they are shredded first).

8. Openness

- Organizations must make readily available to individuals specific information about its policies and practices relating to the management of personal information.

- Organizations must be open about their policies and practices with respect to the management of personal information. Individuals must be able to acquire information about an organization's policies and practices without unreasonable effort. This information must be made available in a form that is generally understandable.

  ***Illustrative Example*:** Tell the receptionist who your privacy officer is so clients can easily be informed.

- The information made available must include:

  (a) the name or title, and the address of the privacy officer and to whom complaints or inquiries can be forwarded,
  (b) the means of gaining access to personal information held by the organization,
  (c) a description of the type of personal information held by the organization, including a general account of its use,
  (d) a copy of any brochures or other information that explain the organization's policies, standards, or codes, and
  (e) what personal information is made available to related organizations (e.g., subsidiaries).

- An organization may make information on its policies and practices available in a variety of ways. For example, an organization may choose explain its policies and practices to the public by:

  - making brochures available in its place of business;
  - mailing information to customers;
  - provide website access;
  - establishing a toll-free telephone number.

9. Individual Access

- Upon request, an individual must be informed of the existence, use, and disclosure of his or her personal information and be given access to that information. An individual must be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

  Note: An organization may not always be able to provide access to all the personal information about an individual. However, *exceptions* to this rule *should be limited and specific* (see section V of this Guide "Exceptions"). The reasons for denying access should be provided to the individual upon request.

  Illustrative Example: Providing quick and easy access to individuals who appear to have legitimate corrections to make to their file information – and making those amendments – will save your organization time, expense and trouble in the long run. It will provide you with accurate information which you need to do your job *and* will likely head off a potential complaint to the Commissioner.

- Upon request, an organization must inform an individual whether or not the organization holds personal information about the individual. The organization must allow the individual access to this information. In addition, the organization must provide an account of the use that has been made of this information and an account of the third parties to which it has been disclosed. An organization may choose to make sensitive medical information available through a medical practitioner.

- An individual may be required to provide sufficient information to permit an organization to provide an account of the existence, use, and disclosure of personal information.

- In providing an account of third parties to which it has disclosed personal information about an individual, an organization should provide a list of the organizations to which it has *actually* disclosed information or at a minimum, a list of the organizations to which it *may* have disclosed information.

  Illustrative Example: If you are unsure about exactly which insurers may have received a client's personal information from your office, instead of providing an exact list, you may provide a list of those insurers likely to have received the information.

- An organization must respond to an individual's request within a reasonable time and at minimal or no cost to the individual. The requested information must be provided or made available in a form that is generally understandable. For example, if the organization uses abbreviations or codes to record information, an explanation must be provided.

Rules for Making a Request

(1) A request must be made in writing.

(2) An organization must assist any individual who informs the organization that they need assistance in preparing a request to the organization.

(3) Time limit – An organization must respond to a request with due diligence and in any case *not later than 30 days after receipt of the request*.

(4) Extension of time limit – An organization may extend the time limit:

(a) for a maximum of 30 days if:

(i) meeting the time limit would unreasonably interfere with the activities of the organization, or

(ii) the time required to undertake any consultations necessary to respond to the request would make the time limit impracticable to meet.

or

(b) for the period that is necessary in order to be able to convert the personal information into an alternative format.

In either case, the organization must, *no later than 30 days after the date of the request, send a notice of extension to the individual*, advising them of the new time limit, the reasons for extending the time limit and of their right to make a complaint to the Commissioner in respect of the extension.

(5) Deemed refusal – If the organization fails to respond within the time limit, the organization is deemed to have refused the request.

(6) Costs for responding – An organization may respond to an individual's request at a cost to the individual only if:

(a) the organization has informed the individual of the approximate cost, and
(b) the individual has advised the organization that the request is not being withdrawn.

(7) Reasons – An organization that responds within the time limit and refuses a request must inform the individual in writing of the refusal, setting out the reasons and any recourse that they may have under this part of the Act (i.e., indicating that they may file a complaint with the Privacy Commissioner within *6 months* of the refusal).

(8) Retention of information – an organization that has personal information that is the subject of a request must retain the information for as long as is necessary to allow the individual to exhaust any recourse under that they may have under the Act.

- When an individual successfully demonstrates the inaccuracy or incompleteness of personal information, the organization must amend the information as required. This may involve the correction, deletion, or addition of information. Where appropriate, the amended information must be transmitted to third parties having access to the information in question (e.g., such as insurance companies).

- When a challenge is not resolved to the satisfaction of the individual, the substance of the unresolved challenge must be recorded by the organization. When appropriate, the existence of the unresolved challenge is to be transmitted to third parties having access to the information in question.

10. Challenging Compliance

- An individual must be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.

- Organizations must implement accessible and simple procedures to receive and respond to complaints or inquiries about their policies and practices relating to the handling of personal information.

  Illustrative Example: Create a simple-to-use complaint form which requires individuals to provide basic information and describe the nature of their complaint.

- Organizations must inform individuals who make inquiries or lodge complaints of the existence of relevant complaint procedures.

- An organization must investigate all complaints. If a complaint is found to be justified, the organization must take appropriate measures, including, if necessary, amending its policies and practices.

  Illustrative Example: Clearly document all complaints and your organization's actions in response to individual complaints, by noting these details in the client's file and also in a master privacy file.

Note: To find out more about the process for challenging compliance and about the role of the Privacy Commissioner, you should contact the Office of the Privacy Commissioner at 1-800-282-1376 or go to their website at www.privcom.gc.ca.

V Exceptions

When is consent not required? Here are some relevant examples: (Note: This list is not exhaustive).

Collection Without Knowledge Or Consent

- It is in the interests of the individual and consent cannot be obtained in a timely way.
- For purposes related to investigating a breach of an agreement or a contravention of the laws of Canada or a province and the availability or the accuracy of the information would otherwise be compromised.
- The information is publicly available and is specified by the regulations under the Act. ***Use Without Knowledge Or Consent***
- There are reasonable grounds to believe the information could be useful in the investigation of a contravention of the laws of Canada, a province or a foreign jurisdiction.
- The information is used in respect of an emergency that threatens the life, health or security of an individual.

Disclosure Without Knowledge Or Consent

- May be made to a barrister or solicitor (or to an advocate or notary in Quebec) who is representing the organization.
- May be made for the purpose of collecting a debt owed by the individual to the organization.
- Is required to comply with a subpoena or warrant or an order made by a court or other body with jurisdiction to compel the production of information, or to comply with rules of court relating to the production of records.
- Is made on the initiative of the organization to an investigative body or a government institution and the organization has reasonable grounds to believe that the information relates to a breach of an agreement or a contravention of the laws of Canada, a province or a foreign jurisdiction (or in relation to a matter of national security or defence).
- Made to a person who needs the information because of an emergency that threatens the life, health or security of an individual and, if the individual whom the information is about is alive, the organization informs that individual in writing without delay of the disclosure.
- Is made after the *earlier* of:
  (i) 100 years after the record containing the information was created, and
  (ii) 20 years after the death of the individual whom the information is about.

- Concerns information that is publicly available and is specified by the regulations under the Act.

- Is made on the initiative of an investigative body for purposes related to investigating a breach of an agreement or a contravention of the laws of Canada or a province.

- Is required by law.

When can access be refused?

- An organization must not give an individual access to personal information if doing so would likely reveal personal information about a third party – unless the third party consents to the access – or the individual needs the information because a person's life, health or security is threatened.

  Illustrative Example: A person is injured in a slip and fall at your client's home. The injured person has made a claim against the insurance policy. Now the client has requested access to his or her file. If the file also contains personal information, such as a medical report about the injured party, you will have to first obtain consent from the injured person to allow your client access to that medical report.

- An organization is not required to give access to personal information if:

  (a) the information is protected by solicitor-client privilege,
  (b) to do so would reveal confidential commercial information,
  (c) to do so could reasonably be expected to threaten the life or security of another individual,
  (d) the information was collected for purposes related to investigating a breach of an agreement or a contravention of the laws of Canada or a province, or
  (e) the information was generated in the course of a formal dispute resolution process.

VI Conclusion

Insurance brokers should try to comply as best they can with the Act. The actions of your organization are likely to be assessed by clients, other organizations and the general public. As the Act is relatively general in nature, the question of whether a broker has breached the Act is likely to be resolved by whether a broker has made *reasonable* efforts to comply. If you have any questions or doubt as to your legal obligations under this or any other legislation, legal advice from a qualified lawyer should be sought. Additionally, you may wish to contact the Office of the Privacy Commissioner at 1-800-282-1376.

PRIVACY QUESTIONNAIRE[1]

Personal Information Holdings

- Do you know what personal information is?
- Do you collect, use or disclose personal information in your day-to-day commercial activities?
- Do you have an inventory of your personal information holdings?
- Do you know where personal information is held (physical locations and files)?
- Do you know in what format(s) the personal information is kept electronic, paper, etc.)?
- Do you know who has access to personal information in and outside your organization?

Accountability of Organization and Staff

- Have you named a privacy officer who is responsible for your organization's overall compliance with the Act?
- Is this responsibility shared with more than one person?
- If these responsibilities are shared, have they been clearly identified?
- Can your staff respond to internal and external privacy questions on behalf of the organization, or do they know who should respond?
- Does your staff know who receives and responds to:
  - requests for personal information?
  - requests for correction?
  - complaints from the public?
- Do your customers know whom to contact:
  - for general inquiries regarding their personal information?
  - to request their personal information?
  - to request corrections to their personal information?
  - for complaints?
- Is your privacy officer able to explain to the public the steps and procedures for requesting personal information and filing complaints?
- Has your staff been trained on the Act?
- Will there be ongoing training?
- Is your staff able to explain the purposes for the collection, use and disclosure of personal information to customers in easy to understand terms?
- Is your staff able to explain to customers when and how they may withdraw consent and what the consequences, if any, there are of such a withdrawal?
- Will you inform your employees of new privacy issues raised by technological changes, internal reviews, public complaints and decisions of the courts?

---

1 This Questionnaire is from the document, *Your Privacy Responsibilities: A Guide for Businesses and Organizations to the Personal Information Protection and Electronic Documents Act,* produced by the Office of the Privacy Commissioner and is used with permission.

Information for Customers & Employees

- ❑ Do you have documents that explain your personal information practices and procedures to your customers?
- ❑ Does this information include how to:
  - obtain personal information?
  - correct personal information?
  - make an inquiry or complaint?
- ❑ Does this information describe personal information that is:
  - held by the organization and how it is used?
  - disclosed to subsidiaries and other third parties?
- ❑ Do you have a privacy policy for your web site?
- ❑ Is your privacy policy prominent and easy to find? Is it easily understandable?
- ❑ Do your application forms, questionnaires, survey forms, pamphlets and brochures clearly state the purposes for the collection, use or disclosure of personal information?
- ❑ Have you reviewed all your public information material to ensure that any sections concerning personal information are clear and understandable?
- ❑ Have you ensured that the public can obtain this information easily and without cost?
- ❑ Is this information reviewed regularly to ensure that it is accurate, complete and up to date?
- ❑ Does this information include the current name or title of the person who is responsible for overseeing compliance with the Act?

Limiting Collection, Use, Disclosure and Retention to Identified Purposes

- ❑ Have you identified the purposes for collecting personal information?
- ❑ Are these purposes identified at or before the time the information is collected?
- ❑ Do you collect only the personal information needed for identified purposes?
- ❑ Do you document the purposes for which personal information is collected?
- ❑ If you gather and combine personal information from more than one source, do you ensure that the original purposes have not changed?
- ❑ Have you developed a timetable for retaining and disposing of personal information?
- ❑ When you no longer require personal information for the identified purposes or it is no longer required by law, do you destroy, erase or make it anonymous?

Consent

- ❑ Does your staff know that an individual's consent must be obtained before or at the time they collect personal information?
- ❑ Does your staff know they must obtain an individual's consent before any new use or new disclosure of the information?
- ❑ Do you use express consent whenever possible, and in all cases where the information is sensitive or the individual would reasonably expect it?
- ❑ Is your consent statement worded clearly, so that an individual can understand the purpose of the collection, use or disclosure?

- Do you make it clear to customers that they need not provide personal information that is not essential to the purpose of the collection, use or disclosure?

Third Party Transfers

- Do you use contracts to ensure the protection of personal information transferred to a third party for processing?
- Does the contract limit the third party's use of information to purposes necessary to fulfil the contract?
- Does the contract require the third party to refer any requests for access or complaints about the information transferred to you?
- Does the contract specify how and when a third party is to dispose of or return any personal information it receives?

Ensuring Accuracy

- Is personal information sufficiently accurate, complete and up to date to minimize the possibility that your organization might use inappropriate information?
- Does your organization document when and how personal information is updated, to ensure its accuracy?
- Do you ensure that personal information received from a third party is accurate and complete?

Safeguards

- Have you reviewed your physical, technological and organizational security measures?
- Do they prevent improper access, modification, collection, use, disclosure and/or disposal of personal information?
- Is personal information protected by security safeguards that are appropriate to the:
  - sensitivity of the information?
  - scale of distribution?
  - format of the information?
  - method of storage?
- Have you developed a "need-to-know" test to limit access to personal information to what is necessary to perform assigned functions?
- Has your staff been trained about security practices to protect personal information? For example, is staff aware that personal information should not be left displayed on their computer screens or desktops in their absence?
- Is your staff aware that they should properly identify individuals and establish their right to access the personal information before disclosing it?
- Do you have rules about who is permitted to add, change or delete personal information?
- Is there a records management system that assigns user accounts, access rights and security authorizations?
- Do you ensure that no unauthorized parties may dispose of, obtain access to, modify or destroy personal information?

Requests for Access to Personal Information

- Is your staff aware of the time limits the law allows to respond to access requests?
- Can you retrieve personal information to respond to individual access requests with a minimal disruption to operations?
- Do your information systems facilitate the retrieval and accurate reporting of an individual's personal information, including disclosures to third party organizations?
- Do you provide personal information to the individual at minimal or no cost?
- Do you advise requesters of costs, if any, before personal information is retrieved?
- Do you record an individual's response to being notified of the cost of retrieving personal information?
- Do you provide personal information in a form that is generally understandable? (For example, do you explain abbreviations?)
- Does your organization have procedures for responding to requests for personal information in an alternate format (such as Braille or audio tapes)?

Handling Complaints

- Can an individual easily find out how to file a complaint with you?
- Do you deal with complaints in a timely fashion?
- Do you investigate all complaints received?
- Are your customer assistance and other front-line staff able to distinguish a complaint under the law from a general inquiry? If unsure, do they discuss this with the individual?
- Do you advise individuals about all available avenues of complaints, including the Privacy Commissioner of Canada?
- Are staff responses to public inquiries, requests and complaints reviewed to ensure they are handled fairly, accurately and quickly?
- When a complaint is found to be justified, do you take appropriate corrective measures, such as amending your policies and advising staff of the outcome?