

PIPEDA – Guideline

1. Introduction

As of January 1, 2004 most organizations in Canada have been subject to the *Personal Information Protection and Electronic Documents Act* (PIPEDA) if they conduct commercial activities. PIPEDA represents a new privacy order for the private sector. As public practitioners across Canada conduct commercial activities, they will all be subject to certain provisions of PIPEDA. This guideline is intended to provide guidance to practitioners on how they can comply with the requirements of PIPEDA. It is intended as a “tool” since each practitioner will have to analyze their own personal information management practices and adapt the recommendations to their particular situation.

To ensure that your privacy regime meets the principles embodied in PIPEDA it is important to understand what PIPEDA is trying to accomplish. The right of privacy of an individual is generally considered to be the right of that individual to control information about themselves. This control extends to the individual’s right to exert control over the use and circulation of that information as well.

The term *privacy* is often confused with the term *confidentiality*. As CGA public practitioners are bound to maintain the *confidentiality* of client information pursuant to the Code of Ethical Principles and Rules of Conduct (CEPROC), you might think that you already have the procedures in place to be compliant with the requirements of PIPEDA. The procedures that you already have in place will be helpful, but likely not sufficient to meet the requirements of PIPEDA. This is due in part to the fact that PIPEDA’s requirements will extend beyond client information and may govern the personal information of any staff you might have also. Additionally, *privacy* is a much broader *right* than *confidentiality* because it is an individual’s right to control access to themselves and information about themselves. This includes the collection, use and disclosure of that information. *Confidentiality* is a person’s obligation to protect another individual’s personal information when it is in their possession. It is an obligation to maintain the secrecy of that information and not to misuse or wrongfully disclose it. Because PIPEDA requires the practitioner to ensure the rights of the individual are protected in relation to their personal information, the practitioner’s obligations will go beyond that which is required under the principle of confidentiality.

This guideline will begin with a discussion of the background of privacy legislation around the world and specifically the new PIPEDA in Canada. It will then address each of the 10 guiding principles contained in PIPEDA. It will then move into the “tools” that CGA-Canada has developed for your use in establishing a privacy regime. Finally, it will discuss some other considerations, where to begin, some best practices and templates and a checklist [260] to provide guidance to establish a privacy compliance regime.

It is important to understand that this guideline is intended to provide guidance to the practitioner, not provide legal advice. Dependent upon the nature of your personal information management practices, you should consult legal counsel with an expertise in privacy law compliance to determine that your specific forms of consent or other measures taken to be in compliance with PIPEDA and other applicable laws are appropriate in your specific circumstances.

1.1 Background

Privacy is a significant concern for most Canadians. It has also been a significant concern for individuals in other countries – especially Europe. Sweden was the first European country to pass privacy legislation which it did in 1973. Shortly thereafter it was followed by similar legislation in Germany, Denmark, Norway and France. *The Organization for Economic Cooperation and Development* (OECD), of which Canada is a member, recognized more than twenty years ago that computer technology would create new capabilities to gather and use information. It was felt that this information could easily be exploited so it felt that creating guidelines for the protection of that information was essential. In 1980, the OECD developed a set of guidelines known as the *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. This was the first international standard for protecting the privacy of personal information. The intention of the guideline was to establish harmonization between national privacy legislation while helping to avoid interruptions in the international flow of information. The European Union issued a directive in 1995 that all member countries must ensure their national data protection laws are in compliance with the EU standards. Europe is not alone in

its efforts to protect the privacy of individuals. The United States and Australia are also enacting various pieces of privacy legislation.

The *Canadian Standards Association (CSA)* developed a voluntary privacy code in 1996 based on the OECD privacy guidelines. The CSA code established several principles regarding an individual's right to privacy over their personal information. It proposed that individuals have the right to know what personal information about them is being collected, used and disclosed. It also stated that individuals should have the right to know who is collecting their personal information and for what purpose; the right to reasonably limit the collection, use and disclosure of their personal information through the use of consent and the right to access the personal information held to ensure its accuracy. The CSA code also made organizations responsible for the information they collected and used. Finally, the CSA code stipulated that organizations should be open about their information management practices.

The CSA code provides the foundation for Canada's new PIPEDA. While the CSA code was a voluntary measure organizations could enforce, PIPEDA is required by law.

1.2 The Act

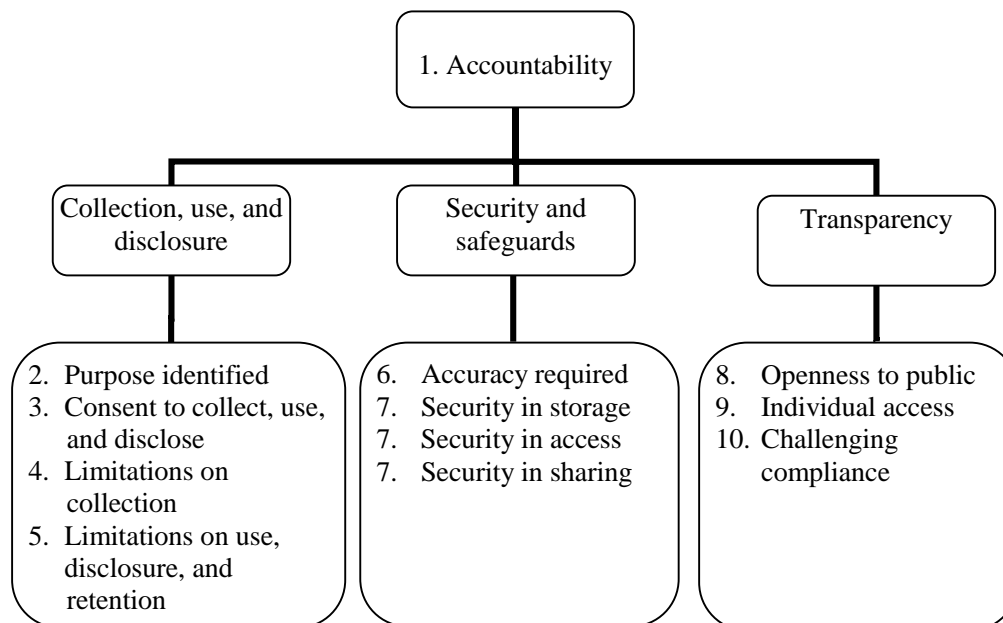
PIPEDA initially came into force on January 1, 2001 and had a three-year phase in period. It was initially applicable to organizations that were generally subject to federal legislative authority. These included organizations such as railways, cable operators, airports and airlines, radio and television broadcasting undertakings, inter-provincial and international shipping and banks. PIPEDA also applied as of January 1, 2001 to organizations that disclose personal information across provincial or international borders for consideration. As of January 1, 2004 the three-year phase in period ended and every organization in Canada that conducts commercial activities is subject to PIPEDA, except within provinces that have "substantially similar" legislation in force. The purpose of PIPEDA is to establish, in an era in which technology increasingly facilitates the circulation and exchange of information, rules to govern the collection, use and disclosure of personal information in a manner that recognizes the right to privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances. Generally, PIPEDA requires that personal information be collected, used and disclosed with the knowledge and consent of the individual to whom it applies.

PIPEDA establishes 10 principles which have to be embodied in every organization's privacy regime in order for the organization to be in compliance. The 10 principles are:

1. Accountability
2. Identify purpose of collection
3. Consent for collection
4. Limiting collection
5. Limiting use, retention, and disclosure
6. Accuracy
7. Security safeguards
8. Openness (to individuals seeking information)
9. Individual access
10. Ability to challenge compliance

The 10 principles can be broadly categorized by their purpose. Under the general purpose of the organization being "*accountable*" come the three categories of "*collection, use, & disclosure*", "*security and safeguards*", and "*transparency*". Illustration 1 depicts these categories and which of the 10 principles applies within that category.

Illustration 1



Some organizations believe they can meet the obligations of PIPEDA just by having a Privacy Code. This is not the case as PIPEDA contains rules that relate to “ongoing” management of personal information. An organization’s practices must evolve to meet changing business needs, customer expectations, information technology advances and interpretations of PIPEDA and other applicable laws by the courts and the Privacy Commissioner of Canada.

1.3 Who does it cover

PIPEDA applies to every organization in Canada that collects, uses or discloses personal information in the course of commercial activities, except within provinces that have "substantially similar" legislation in force. The term “Organization” includes persons, corporations, associations, partnerships, and trade unions. Because public practitioners carry out commercial activities, they are covered by PIPEDA no matter what their type of formation – i.e., proprietorship, limited liability or general partnership, professional corporation or association.

1.4 What does it cover

PIPEDA applies specifically to “personal information”. This term is broadly defined to mean any information about an identifiable individual. However, it does not include business contact information such as the name, title, business address, or telephone number of an employee of an organization.

Personal information includes (but is not limited to):

- name, address, age, marital status, ethnic origin,
- financial information, including credit or loan records and investment holdings,
- employee records including performance evaluations, disciplinary actions, etc.,
- health information,
- opinions, and
- association with a particular organization or activity.

Most public sector privacy laws apply to “recorded” information only. This is not the case with PIPEDA. PIPEDA is not restricted to recorded information only. PIPEDA also requires that personal information be collected, used, or disclosed solely with the knowledge and consent of the individual to whom it pertains. Organizations must also comply with obligations regarding how personal information can be collected, used, and disclosed. These obligations are set out in the 10 principles for privacy compliance which are discussed in detail in the next section.

PIPEDA provides no “grandfathering” exemption so it applies equally to personal information collected prior to January 1, 2004. This means that personal information you already have on file will require the individual’s consent if you are going to use or disclose it for any purpose other than the identified purpose for which it was originally collected.

Certain information and activities are specifically exempted from the requirements of PIPEDA. These are:

- publicly available information, as designated in the Regulations to PIPEDA,
- activities of organizations in provinces that have “substantially similar” legislation in force,
- personal information for personal or domestic use (i.e., holiday card list),
- personal information used solely for journalistic, artistic, or literary purposes, and
- government institutions that fall under existing federal *Privacy Act*.

The exemption for activities of organizations in provinces that have “substantially similar” legislation only applies to activities conducted “within” that Province. Any flow of personal information that is “inter-provincial or international” (meaning crossing Provincial or International boundaries) will still be covered by PIPEDA. In order for Provincial legislation to be “substantially similar” it must, at a minimum, contain the same type of provisions as PIPEDA. What this means is that the policies and procedures required under PIPEDA should generally be required for organizations in Provinces that have “substantially similar” legislation as well. Additionally, if you have any “inter-provincial and/or international” transfers and/or disclosures of personal information, they are subject to PIPEDA so it is in your best interests to establish a privacy regime based on PIPEDA even if you are in a Province that has “substantially similar” legislation. This will help ensure that your privacy requirements are met in all circumstances.

1.5 Failure to comply

PIPEDA gives strong powers to the Office of the Privacy Commissioner of Canada (OPC). The OPC is mandated to receive complaints, conduct investigations, issue reports, publicize findings and may request a hearing in federal court after its report is issued. If you are found to not be in compliance with the legislation you can face fines of up to \$100,000 and a Federal court can order a correction of practices and/or award damages to a complainant (including for humiliation). The OPC has significant enforcement mechanisms including an ability to make public the names of organizations that are subject to investigation.

2. The 10 guiding principles

The Canadian Standards Association (CSA) developed a voluntary privacy code in 1996 based on the OECD privacy guidelines. The CSA code established several principles regarding an individual’s right to privacy over their personal information. It proposed that individuals have the right to know what personal information about them is being collected, used, and disclosed. It also stated that individuals should have the right to know who is collecting their personal information and for what purpose; the right to reasonably limit the collection, use, and disclosure of their personal information through the use of consent and the right to access the personal information held to ensure its accuracy. The CSA code also made organizations responsible for the personal information they collected and used. Finally, the CSA code stipulated that organizations should be open about their personal information management practices. The CSA code provides the foundation for PIPEDA. PIPEDA has 10 separate principles that have to be embodied in every organization’s privacy regime in order for them to be in compliance. This section will discuss each of those 10 principles and provide some suggestions for compliance. In each section on the principles, the term “organization” is to mean practitioner or firm.

2.1 Accountability (Principle 1)

The first principle stated by PIPEDA is the principle of *accountability*. This principle requires organizational accountability for personal information under its control. The organization must designate an individual as its *Privacy Officer* and the identity of that individual must be made known upon request. The organization should ensure that the Privacy Officer has the authority and support to carry out their duties of ensuring the organization establishes and maintains a compliant personal information management system.

An organization is responsible for all personal information in its possession or control, including information it has transferred to a third party for processing. The organization shall use contractual or other means to ensure the third party provides an equal level of protection while the information is in the possession or control of the third party for processing.

The organization must analyze all its personal information handling practices and develop policies and procedures to protect personal information it has in its possession or control. The policies and procedures should guide the organization to:

- protect personal information,
- receive and respond to complaints and inquiries,
- train staff and communicate to staff information about the organization's policies and procedures for the protection of personal information, and
- develop information for clients and others whose personal information you have in your possession or control that explains the organization's policies and procedures for the protection of their personal information.

The principle of accountability is the overriding principle under which all the other principles are given effect. There are risks that the organization can face if it does not undertake to ensure that it meets the objectives of PIPEDA and its principles. If the organization does not have effective accountability regime personal information might be improperly managed. This can potentially result in damage to the organization's reputation and other business relationships because it will be seen as an organization that does not protect the personal information it collects, uses, and discloses. It can also face an investigation by the Office of the Privacy Commissioner who can publish the fact that the organization is under investigation for alleged breaches. This can also damage the reputation of the organization and if the complainant or the Office of the Privacy Commissioner takes the matter to Federal court, it can result in fines.

2.2 Identifying the purpose (Principle 2)

Pursuant to the principle of **identifying purpose**, you must identify the reason(s) for collecting personal information before or at the time of collection. You must also disclose how it will be used and to whom it might be disclosed. Depending on how you collect the information, this notification can be done orally or in writing.

If new purposes are identified after the collection of the personal information, you must obtain the consent of the individual before using the information for the newly identified purpose. For example, if you decide to use client names and addresses to market a new service you are providing and you did not identify this as a reason for collecting the information at the time you collected it, you must obtain the consent of the individual before you can use it for that purpose.

In light of the need to obtain consent when new purposes are identified you should undertake to identify as many purposes for the use of the information at the time you initially collect it. The purposes should be clearly defined and as narrow as possible so the individual understands how the information will be used or disclosed. You must avoid overly broad purpose statements as they may conflict with the "**knowledge and consent**" principle.

To help meet the obligations of this principle you should review the personal information you currently possess or control and ensure it is all required for a specific purpose. You must also keep in mind that the purpose must meet the "reasonable person test". The purpose must be something that a "reasonable person" would expect under the circumstances. For example, when collecting personal information to prepare a personal tax return, it seems reasonable that you would need the person's financial information, social insurance number, marital status, age, address and medical receipts. It might not seem reasonable to collect information about any associations the individual might be a member of unless they are attempting to deduct dues or fees that were payable to that association. A suggestion for identifying the purpose of information collection in relation to personal tax returns could be to require the "provision of any personal information required to be reported in the individual's personal tax return for the year". Keep in mind that you may need to develop several different "purpose" statements dependent upon the type of engagement you are going to undertake and the type of information that would normally be required or expected to complete the type of engagement.

Consideration should also be given to a purpose clause that states you will use their personal information to identify services that in your professional judgment might be beneficial for them. These services might include estate planning, tax planning, or elder care services. If you already offer a variety of services it is suggested that you list the types of services that might be offered rather than using an overly broad purpose.

The principle risk involved if you do not specify the purpose(s) for which you have collected the personal information is that it may give rise to a complaint of deceptive business practices.

2.3 Consent (Principle 3)

The **consent** principle embodies the rights of individuals to have a choice of whether they want their personal information collected, used, or disclosed and the purposes for which it will be collected, used, or disclosed. Organizations are required to obtain the consent of the individual prior to or at the time the product or service is supplied. The consent must be voluntary on the part of the individual and they have to understand what they are consenting to. They must be provided with the choice of whether their information will be provided to any third parties or will be used for a purpose other than the purpose they expect when providing the information.

Consent can be implied or it can be express. It can be obtained in person, by phone, by mail, by fax, or via the Internet. For example, if a client comes in to have their personal tax return prepared and this is the stated purpose for collecting the personal information, there is implied consent for your disclosure of this information to CCRA because that is the expectation when having a tax return prepared by a professional accountant. However, for you to use that same information for some other purpose, such as marketing a new service, you should obtain express consent since most of the information you collect from clients will be considered sensitive information.

Some personal information is considered more sensitive. Whether the information will be considered sensitive or not will depend on the circumstances under which it is collected. The type of information that is generally considered to be sensitive is financial information, medical or health information, social insurance number, racial or ethnic origin, political opinions, and religious or philosophical beliefs. Where information collected is considered sensitive, the individual should provide express consent if their information is to be disclosed to a third party or used for a purpose other than that for which it was originally collected. If the new purpose is not identified until a later date, the consent can be obtained at that later date. Organizations should treat as “sensitive” any information it receives from a third party that the third party identifies as sensitive. Obtaining express consent from an individual for their sensitive information protects both the individual and the practitioner.

For an individual who is a minor, seriously ill, or mentally incapacitated, consent may be obtained from a legal guardian or other person having a power of attorney for the individual.

The consent obtained will only be meaningful if the individual understands what they have consented to and how their information will be used. Consent clauses should be easy to find and use straightforward language. You should avoid using overly broad purposes because this may impact on the individual’s ability to properly understand what they have consented to.

You may not obtain consent by deceptive means and cannot make consent a condition for supplying the service unless the information requested is required for the specified purpose. For example, if an individual does not consent to providing you with their financial information or social insurance number for purposes of completing their personal tax return, you would be unable to complete the engagement as this information is legislatively required on the tax return. In such circumstances, you would be justified in denying the service if consent is not provided.

Where possible, a signed consent form should be maintained in a client’s permanent file so that you can readily access it if necessary.

CCRA consent forms used for personal or corporate tax returns and e-filing, apply only to authorize you to collect, use, or disclose information with CCRA. They are of limited use for purposes of PIPEDA in general.

When obtaining consent the expectations of the individual must be considered. For example, an individual who subscribes to a magazine should reasonably expect that the organization, in addition to using the individual’s

name and address for mailing and billing purposes, would also contact the person to solicit the renewal of the subscription. In this case, the organization may be safe in assuming that the individual's request constitutes consent for specific purposes. On the other hand, an individual would not reasonably expect that personal information provided to a health care provider would be given to a company selling health care products, unless consent was obtained. For a practitioner who prepares an individual's personal tax return, it appears that it is safe to assume that contacting the individual in the following year to market tax return preparation would be implied in the consent provided to prepare the return in the first year. However, this would not imply that the practitioner could freely market other professional services to the individual unless consent for those purposes was obtained prior to contacting them.

The risks of not obtaining appropriate consent include potential legal liability or sanctions where the obligation to seek consent is required by law or self-regulation. Additionally, if consent is not obtained or is obtained by deceptive means the organization's reputation may suffer as this can be publicly disclosed by the Office of the Privacy Commissioner.

There are some exceptions for the requirement to obtain consent. These are discussed in detail in section 4.2 of this guideline.

Section 5 of this guideline provides further guidance on consent for practitioners.

2.4 Limiting collection (Principle 4)

The *limiting collection* principle states that an organization may not indiscriminately collect personal information. PIPEDA states that both the amount and types of information collected shall be limited to that which is necessary to fulfill the purposes identified. This principle also stipulates once again that you may not deceive or mislead individuals about the reasons for collecting personal information.

You should limit the amount and type of personal information you collect to what is absolutely necessary for the identified purpose(s). By potentially reducing the amount of personal information you collect you may be able to lower your cost of collecting, storing, retaining and archiving that data. It may also reduce your risk of having personal information inappropriately used or disclosed.

2.5 Limiting use, disclosure, and retention (Principle 5)

The *limiting use, disclosure, and retention*, principle states that an organization may not use personal information collected for other than the initially stated purposes. It also states that personal information may not be disclosed to third parties without the individual's consent and that information may only be retained for as long as it is necessary to complete the specified purpose for which it was originally collected. You should adopt policies and procedures for the retention and eventual destruction of any personal information you may have collected, used, or disclosed once it is no longer necessary to maintain that information.

When disposing of information you should ensure that it is disposed of, erased, or made anonymous in such a way that prevents improper access. Shredding paper files or deleting electronic records are recommended. You should also establish a regular retention schedule to ensure that information which is no longer required to be maintained is destroyed. As a matter of guidance, it is generally recommended that tax information be maintained for 6 years after the year to which the information relates. This is a guideline established by CCRA. As such, practitioners who maintain client files for longer than this suggested period may be in breach of this principle unless they can establish that there is a valid reason for holding the information longer. Also, you should ensure that hard drives in computers are reformatted before disposing of them to ensure that no personal data can be obtained from them if there was any personal information stored on them. Other retention periods will depend on the engagement performed and should be determined by the practitioner.

2.6 Accuracy (Principle 6)

The accuracy principle states that an organization must ensure that personal information held is accurate, complete, and up-to-date. The organization must minimize the possibility that incorrect information will be used when making a decision about the individual or disclosing it to a third party. The organization must also provide access to the individual for the information held to ensure that it is accurate and complete.

2.7 Safeguards (Principle 7)

The safeguards principle requires that organizations protect personal information with security safeguards appropriate to the sensitivity of the information. The measures should protect the information against loss, theft, misuse and unauthorized access, disclosure, copying, or modification. This protection is to apply no matter what format the information is held in. You should review and update security measures on a regular basis. Physical measures might include locked filing cabinets, restricting access to offices or alarm systems. Technological measures might include passwords, encryption, virus protection, regular back-ups of data, or firewalls. Finally, organizational controls might include security clearances, limiting access to files and information on a “need-to-know” basis, staff training or confidentiality agreements. It is important to remember that these safeguards are not just to protect the information from “outsiders” gaining access. Consideration should be given to only allowing access to client files to staff or other individuals who need to work on the files. Additionally, staff should not leave client information in plain site when leaving the office if cleaning staff come in during the evening.

You should ensure that staff are well aware of the necessity to not only keep client information confidential (pursuant to CGA Code of Ethical Principles and Rules of Conduct), but also to keep it private.

2.8 Openness (Principle 8)

The *openness* principle requires that an organization make available to individuals whose information is currently held, the organization’s policies and procedures dealing with privacy and the protection of personal information. These policies should be understandable and easily available to anyone requesting a copy. To meet this obligation, organizations must make their employees aware of the procedures for responding to individual inquiries. The types of inquiries employees should be able to respond to include:

- the name or title and address of the person who is accountable for the organization’s privacy policies and procedures (i.e., most likely the Privacy Officer),
- the name or title and address of the person to whom access to information requests should be sent,
- how individuals can access their personal information, and
- how individuals can complain to the organization about privacy related issues.

Organizations should have brochures or other written material that describes their personal information policies. This will be the most efficient way to ensure that individual inquiries can be responded to in an efficient manner.

2.9 Providing access (Principle 9)

The access principle requires that an organization provide access to any individual whose information they possess or control and to correct it if the information is inaccurate or incomplete. When requested, the organization must inform individuals whether they have any personal information about them. You must be able to inform the individual how the information has been used and provide a list of any other organizations to whom the information has been disclosed. This requires you to have a complete history or audit trail or all personal information in your organization’s possession or control.

Requests must be made in writing and the organization must assist the individual if they need help in filling it out the request. The organization may charge a minimal fee, if any, only when they have informed the individual of the approximate cost and the individual does not withdraw the request. When deciding to charge a fee, the organization must be conscientious of the fact that a fee which would be considered too high by a reasonable person might place them in breach of the access principle. In light of this, it is suggested that no fee be charged to show the organization intends to comply with PIPEDA in good faith.

When a request for access is made, the organization must reply with the information no later than 30 days after the request is made and they must use due diligence to reply to the request. There are limited circumstances under which the organization may extend the time frame for an extra 30 days. These circumstances are:

- if meeting the original 30 day time limit would unreasonably interfere with the activities of the organization,
- the time required to undertake any consultations necessary to respond to the request would make the time limit impracticable to meet, and

- if additional time is necessary to convert personal information to an alternate format.

In either case, the organization must, no later than 30 days after the request is made, send a notice of extension to the individual advising of the new time limit, the reasons for extending the time limit and of the individual's right to make a complaint to the Office of the Privacy Commissioner of Canada about the extension. If you fail to respond in the appropriate manner and in the required time frame, the organization will be deemed to have refused the request.

The information you provide to the individual must be understandable. The onus is on the organization to explain any acronyms, abbreviations or codes used. To make it easier for the organization to respond to such requests, it is advisable to keep all personal information in one location or have a record of where the information is stored so retrieval is easier. Never disclose personal information unless you are certain of the identity of the requestor and that person's right to access it.

In certain situations you may deny access to all or some of the personal information held. Exceptions should be limited and specific. The reasons for denying access should be provided to the individual upon request. Exceptions may include information that is prohibitively costly to provide, contains references to other individuals, cannot be disclosed due to legal, security or commercial proprietary reasons, could reasonably be expected to threaten the life or security of another individual, the information was collected with respect to investigating a breach of an agreement or a contravention of law, the information was generated in the course of a formal dispute resolution process, or is subject to solicitor-client or litigation privilege.

2.10 Challenging compliance (Principle 10)

The *challenging compliance* principle gives the individual the right to challenge the organization's compliance with privacy principles. Organizations are required to establish policies and procedures that deal with the receipt and investigation of all complaints or inquiries regarding the organization's policies and procedures relating to the handling of personal information. The complaint procedures should be easy to understand and readily accessible. Your organization is required to investigate all complaints. If a complaint is found to be justified, the organization shall take appropriate measures, including, if necessary, amending its policies and procedures.

You must also inform the individual of the various avenues of recourse that they have. These would include your own complaint procedures as well as those of your regulatory body, if they have any, and the Office of the Privacy Commissioner of Canada. If you are unable to conduct the complaint investigation within your own organization, you should assign it to a person with the skills necessary to conduct such an investigation fairly and impartially.

2.11 Summary

The foregoing 10 principles are all detailed in the PIPEDA legislation. The principles detail the obligations of organizations in relation to an individual's right to know what personal information about them is being collected, used and disclosed. It embodies the principle that individuals should have the right to know who is collecting their personal information and for what purpose; the right to reasonably limit the collection, use and disclosure of their personal information through the use of consent and the right to access the personal information held to ensure its accuracy. In this respect organizations are responsible for the information they collect and use and must be open about their information management practices. These 10 separate principles must be embodied in every organization's privacy regime in order for them to be in compliance.

3. Privacy tools

PIPEDA establishes privacy rules that will apply to all organizations by no later than January 1, 2004. To the extent that your organization collects, uses, and/or discloses personal information in the course of commercial activities, it will be obliged to comply with PIPEDA or "substantially similar" provincial laws. In order to assist CGAs in meeting PIPEDA's obligations, the Association has developed several privacy compliance tools. These tools are all available on the CGA PD Network. The PD Network also contains articles on the topic of Privacy that may assist you in developing your privacy compliance regime. The tools produced by CGA-Canada for your use are:

The CGA Model Privacy Code (Section [220])

The CGA Model Privacy Protection Pledge (Section [230])

The CGA Model Commitment to Privacy (Section [240])

The CGA Model Privacy FAQ (Section [250])

3.1 Legal counsel

This PIPEDA guideline section has been made available to assist CGA practitioners to meet the obligations of new federal privacy legislation, which regulates the collection, use, and disclosure of personal information in commercial activities.

The advice and tools contained herein are intended to serve as guidance only. Your firm's entire privacy compliance should be fully reviewed by legal counsel with expertise in privacy law before CGAs rely or make use of it in relation to their specific situation. Legal advice is dependent upon the particular facts in a particular situation, and the application of the appropriate laws and legal principles to that situation. As a result, CGA associations shall not be liable for any direct, indirect, incidental, consequential, special, punitive, or exemplary losses or damages of any nature or kind whatsoever resulting from a practitioners use of this guideline and the privacy compliance tools.

4. Other considerations

There are a number of areas which require further discussion and which are not contained within the Principles as outlined in Section 2. These areas deal with what your employees need to know and what is the difference between a "transfer" of personal information and a "disclosure" of personal information. These discussions are meant to provide guidance to the practitioner. It is incumbent on each practitioner and firm to determine the appropriate steps to take in order for your firm and privacy regime to comply with the requirements of PIPEDA.

4.1 What do your employees need to know?

Front-line employees are the most likely individuals to get any initial questions regarding the firm's privacy regime. The accountability principle recognizes this and requires that the organization take steps to inform and train staff on the firm's privacy policies and procedures. To help provide guidance on what employees need to know, they should be able to answer the following questions:

1. How do I respond to questions regarding our firm's privacy policies?
2. What is consent? How and when do we obtain it?
3. How do I recognize and process requests for access to personal information?
4. To whom should I refer complaints about privacy matters?
5. What are my own privacy protections and rights?
6. What specific procedures do I need to follow to ensure the protection of personal information?

The answers to these questions may be different in each organization dependent upon particular policies and procedures. As such, you need to establish these policies and procedures before training staff in how to respond to these questions.

4.2 Exception to consent

Within PIPEDA there are certain limited circumstances under which consent will not be necessary for the collection, use, or disclosure of personal information.

The circumstances under which consent is not required for the *collection* of information are:

- The collection is clearly in the interests of the individual and consent cannot be obtained in a timely way;
- The collection is solely for journalistic, artistic or literary purposes;
- The information is publicly available and is specified by the regulations; or
- It is reasonable to expect that the collection with the knowledge or consent of the individual would compromise the availability or the accuracy of the information and the collection is reasonable for purposes related to investigating a breach of an agreement or an actual or potential contravention of the laws of Canada or a Province.

The circumstances under which consent is not required for the *use* of information are:

- For an emergency that threatens the individual's life, health or security;
- For statistical or scholarly study or research (the organization must notify the Privacy Commissioner before using the information);
- The information is publicly available as specified by regulation;
- If the organization has reasonable grounds to believe the information could be useful when investigating a contravention of a federal, provincial, or foreign law and the information is used for that purpose;
- If the use is clearly in the individual's interest and consent is not available in a timely manner;
- If knowledge and consent would compromise the availability or accuracy of the information, and collection was required to investigate a breach of an agreement or an actual or potential contravention of the laws of Canada or a Province.

The circumstances under which consent is not required for the *disclosure* of information are:

- To a lawyer representing the organization;
- To collect a debt the individual owes to the organization;
- To comply with a subpoena, warrant, or order made by a court or other body with appropriate jurisdiction;
- To a government institution that has requested the information, identified its lawful authority, and indicated that disclosure is for the purpose of enforcing, carrying out an investigation, or gathering intelligence relating to any federal, provincial, or foreign law; or suspects that the information relates to national security or the conduct of international affairs; or is for the purpose of administering any federal or provincial law;
- To an investigative body named in the Regulations of the Act or government institution when the organization itself believes the information concerns a breach of an agreement, or an actual or potential contravention of a federal, provincial, or foreign law, or suspects that the information relates to national security or the conduct of international affairs;
- If made by an investigative body for the purposes related to the investigation of a breach of an agreement or an actual or potential contravention of a federal or provincial law;
- In an emergency that threatens the individual's life, health, or security (the organization must inform the individual of the disclosure);
- For statistical or scholarly study or research (the organization must notify the Privacy Commissioner before disclosing the information);
- 20 years after the individual's death or 100 years after the record was created;
- If it is publicly available as specified by regulation;
- If required by law.

4.2 **Transfer or disclosure of information**

CGA practitioners may have several different relationships with their clients. They may act as third party processors of information, for example when they provide payroll services or records creation. They may also act independently of the client, for example when providing assurance type services such as audits or review engagements. The distinction of what type of relationship exists in any engagement because as a third party processor you are effectively acting as an agent of the client while in assurance engagements you want to maintain your independence so you cannot be an agent of your client. When you are acting as an "agent" for your client the information coming from the client will normally be considered a "transfer" while the flow of information from a client when you are acting independently will normally be considered a "disclosure". In regards to PIPEDA this distinction is important because PIPEDA deals with "transfers" of information differently than it does with "disclosures".

Generally, an organization must have the consent of the individual for the "disclosure" of their personal information to a third party. It is also generally understood that PIPEDA allows an organization to "transfer" personal information to a third party without consent for processing purposes. Transfers are only allowed for limited purposes and they are subject to stringent conditions. For instance, the third party processor can only use the information for the specified purpose and has to protect the information as required by PIPEDA. In situations where the CGA is acting as an agent of the client and the information is being transferred to them, consent from the individual is not required to be obtained by the CGA. Despite this, PIPEDA's requirements must still be met by the CGA. Pursuant to PIPEDA, an organization is responsible for personal information in

its possession or custody, including information that has been transferred to a third party for processing. The organization shall use contractual or other means to provide a comparable level of protection while the information is being processed by the third party. This means the CGA will have to meet all the other requirements of PIPEDA, except for the consent to collect the information.

CGA practitioners should normally have an agreement or engagement contract with the client when performing work in an agency type capacity. Due to the requirements of PIPEDA, this may become standard practice for all organizations using agents as PIPEDA requires that an organization shall use contractual or other means to ensure the third party provides an equal level of protection while the information is in the possession or control of the third party for processing (Principle 1 – Accountability). This contract will generally formalize the “agency” relationship between the CGA and the client. When the CGA has such a relationship, they should ensure that the client has the proper consent to allow for the transfer of the information to them for processing.

If the CGA is acting independently of the client, for example in an assurance type engagement, the information flow will generally be considered a “disclosure” of information by the client and a “collection” of information by the CGA. It may be difficult or impractical for the CGA to obtain consent directly from the individuals whose personal information is being collected as part of the engagement because they are not normally a party to the engagement contract – for example, payroll information, tenant lists for rental properties or loans payable or receivable. In such situations it appears to be more appropriate for the client to obtain the necessary consent from the individuals for the practitioner to use it. To avoid any misunderstandings, responsibility for obtaining this consent should be set out in the engagement contract between the CGA and the client and the CGA should not undertake to collect or use such personal information unless they are satisfied that such consent has been obtained.

5. Templates and best practices

This section provides sample wording for engagement letters and consent forms. These are suggestions and you should analyse your own circumstances and determine what is most appropriate. The sections that deal with suggested best practices are meant for guidance only. In all situations your own professional judgment, and that of your legal counsel, should be exercised to determine whether your information practices are in compliance with the requirements of PIPEDA.

5.1 Sample engagement letter wording

It is expected that you adopt wording on PIPEDA for all engagement contracts such as:

[*Client name*] acknowledges that [*CGA firm*] will have access to all personal information that is required to complete our engagement. Our services are provided on the basis that:

- you represent to us that you have obtained any required consents for the collection, use, and disclosure to us of personal information required under applicable privacy legislation; and
- we will retain all personal information in compliance with our Privacy Code.

5.2 Sample consent form language

As previously noted in section 2.3, the consent principle embodies the rights of individuals to have a choice of whether they want their personal information collected, used, or disclosed and the purposes for which it will be collected, used, or disclosed. Organizations are required to obtain the consent of the individual prior to or at the time the product or service is supplied. The consent must be voluntary on the part of the individual and they have to understand what they are consenting to. They must be provided with the choice of whether their information will be provided to any third parties or will be used for a purpose other than the purpose they expect when providing the information.

Consent can be implied or it can be express. It can be obtained in person, by phone, by mail, by fax, or via the internet. Some personal information is considered more sensitive. The type of information that is generally considered to be sensitive is financial information, medical or health information, social insurance number, racial or ethnic origin, political opinions, and religious or philosophical beliefs. Where information collected is considered sensitive, the individual should provide express consent if their information is to be disclosed to a third party or used for a purpose other than that for which it was originally collected. In light of the fact that the vast majority of information to be collected by the CGA will be considered sensitive, strong consideration should be given to having all clients provide express (written) consent to having their personal information

collected, used and disclosed. This can be obtained in the form of an engagement letter or a stand-alone consent form. Some suggested wording for the consent form would be as follows:

[*Client name*] acknowledges that [*CGA firm*] will be collecting and using my personal information for the following purposes:

- preparation of personal tax return,
- preparation of personal financial plan,
- provision of income tax advice,
- provision of estate planning advice, and/or
- marketing of other professional services offered by [*CGA firm*]

I hereby further acknowledge that disclosure of this information may be made to the following third parties:

- Canada Customs and Revenue Agency,
- respective provincial tax authorities,
- personal bank manager,
- legal counsel,
- insurance agent, and/or
- other professional(s) or third-party processors as required by the nature of the engagement.

I acknowledge that [*CGA firm*] owes me a professional duty to maintain the confidentiality of my personal information as well as to protect my personal information pursuant to PIPEDA. In light of these obligations I hereby consent to the use of [*CGA firm's*] professional judgment regarding the use of other professional(s) or third-party processors that may be required to complete the engagement I have retained them for. Disclosure to other parties, including my bank manager, legal counsel, or insurance agent may be made when directed by me to do so.

The above list and separate references in the closing paragraph would be modified by the CGA dependent upon what types of services they perform and to whom they expect disclosure may be made. You could allow for each service offered or potential disclosure to be made to be consented to separately or not consented to by using a “check the box” (opt-in) type of consent. Keep in mind that all other aspects of the Privacy principles should be embodied in your privacy regime so you may want to add statements regarding the limiting of collection, etc.

5.3 Best practices during tax time

Tax time for many practitioners is a very busy time of year during which you will be collecting, using, and potentially disclosing a great deal of personal information. Some suggestions for best practices to be followed during this time of year are:

- Ensure staff and any sub-contractors you may use are completely familiar with your privacy policies and procedures.
- Ensure that only information which is necessary for the completion of the tax returns is collected.
- Ensure that only those individuals actually working on a particular tax return have access to the personal information contained in the tax return or the client file. If using a network, utilize password access to the client files to protect against unauthorized access.
- Obtain express consent from the individual for the collection, use, and disclosure of their personal information.
- Ensure that any draft copies of tax returns prepared are properly destroyed. Disposing of papers that contain personal information in the normal garbage would likely be considered a very dangerous practice and in breach of the “security” principle. Consider shredding of all papers during tax season that are not necessary.
- Facsimiles and e-mails may not be considered to be secure forms of data transmission. As a result, if you plan to use either form for communicating with your client or other third parties, ensure they are encrypted or the information is made anonymous. Personal information is only subject to PIPEDA when it can be linked to an identifiable individual.

- If your client decides to communicate personal information to you via e-mail or fax they have likely assumed the risk of the security principle in relation to that information. You should be careful about replying or forwarding such e-mails in light of the point above if you include any of the original e-mail in your reply.
- When sending e-mails to multiple parties, bear in mind that e-mail addresses may be considered personal information depending on the circumstances. As such, the “bcc” address line should be used to protect the privacy of the addresses of others on the distribution list.

5.4 Best practices on assurance engagements

When conducting assurance engagements most of the personal information you will collect, use or disclose will be information about third party individuals that the client has collected. For example, payroll information, tenant information for leasing companies, and accounts receivable or payable details for most businesses where the accounts receivable or payable are from or to an individual. Since we have already established that when conducting assurance engagements, you are not acting in the capacity of an agent, consent issues will arise. Best practices to utilize in regards to the personal information that might be collected, used, or disclosed during an assurance engagement are:

- Ensure staff and any sub-contractors you may use are completely familiar with your privacy policies and procedures.
- Ensure that only information which is necessary for the completion of the engagement is collected.
- Ensure that only those individuals actually working on the file have access to the personal information contained in the client file. If using a network, utilize password access to the client files to protect against unauthorized access.
- Ensure that any draft copies of tax returns that may be prepared as part of the engagement are properly destroyed. Disposing of papers that contain personal information in the normal garbage would likely be considered a very dangerous practice and in breach of the “security” principle. Consider shredding all documents not retained in the client file.
- Facsimiles and e-mails may not be considered to be secure forms of data transmission. As a result, if you plan to use either form for communicating with your client or other third parties, ensure they are encrypted or the information is made anonymous. Personal information is only subject to PIPEDA when it can be linked to an identifiable individual.
- If your client decides to communicate personal information to you via e-mail or fax they may have likely assumed the risk of the security principle in relation to that information. You should be careful about replying or forwarding such e-mails in light of the point above if you include any of the original e-mail in your reply.
- When sending e-mails to multiple parties, bear in mind that e-mail addresses may be considered personal information. As such, the “bcc” address line should be used to protect the privacy of the addresses of others on the distribution list.
- Ensure engagement contracts adequately address (among other things) the issue of consent and the responsibility for obtaining the necessary consent.
- If your client determines that it does not have the necessary consent to enable you to use the information for your engagement you should first request that the client obtain the specific consent necessary. If they are unable to do that you will need to consider this limitation on the scope of your engagement in your engagement report.
- Only collect and document personal information that is necessary to complete the engagement.
- If practical, make the personal information anonymous when you record or document it. For example, if you must use personal information to ascertain whether a particular loan is collectible or not, you can document the procedure by referencing the loan number rather than the individual’s name. Personal information is only subject to PIPEDA when it can be linked to an “identifiable” individual.
- Ensure your file retention policies adequately address the limitations placed on retaining personal information and it is followed to ensure files are destroyed that are no longer necessary to be held.