CANADIAN
MARKETING
ASSOCIATION
CMA

ACM
ASSOCIATION
CANADIENNE
du MARKETING

# Canadian Privacy Legislation Compliance Guide

## for Members of the Canadian Marketing Association

# Canadian Privacy Legislation Compliance Guide
## for Members of the Canadian Marketing Association

## Introduction

This document contains information on implementing the federal government's ***Personal Information Protection and Electronic Documents Act*** (PIPEDA) for members of the Canadian Marketing Association.

Like CMA's own Privacy Code, the federal law addresses major themes, the collection, use and disclosure of personal information - and is structured according to basic principles.

On January 1, 2004, privacy laws came into force across Canada governing all commercial transactions in the country. PIPEDA applies in seven provinces, including Ontario, and when personal information is disclosed across a provincial or international boundary for consideration. British Columbia, Alberta and Quebec have their own privacy legislation, which apply to personal information collected, used and/or disclosed within those provinces.

Schedule 1 of PIPEDA contains the 10 privacy principles of the Canadian Standards Association's (CSA) Model Code for the Protection of Personal Information (see page 5). Like the CMA Privacy Code, the CSA principles have their roots in the 1984 treaty reached by the Organization for Economic Cooperation and Development (OECD).

While privacy laws now supersede the 10 CSA principles, the federal, B.C. and Alberta laws have all adopted the CSA principles as the basis for their own legislation. The differences between the CSA Code, PIPEDA and the laws in B.C. and Alberta are minor and largely confined to a series of explanatory notes in the CSA document, which are not incorporated in the law. Where appropriate, the issues addressed in the notes are discussed in the commentary that follows in this guide.

For the purposes of this guide, the focus will be on the federal law, PIPEDA. The federal law is composed of two main parts, the main statutory act and a detailed Schedule 1 (referenced previously), which contains the operative sections with which marketers will be most concerned.

### How the Law Applies

The law applies to commercial transactions using personal information. Personal information is "information about an identifiable individual," and includes things such as name, address, purchase habits, age or gender. There is a limited exemption for business contact information (name, title or business address and telephone number of an employee of an organization). The law requires appropriate consent for the collection, use and disclosure of personal information in the course of commercial activities.

For most organizations, the law is far-reaching and applies to every area of their information-gathering and handling practices. For example, it applies to situations as simple as sending a mailing label across provincial borders – this will impact a very large number of marketers and suppliers across the country.

Marketers are therefore advised that the prudent course of action will be to assume that the law covers their operations and to ensure their organizations comply with its requirements.

## New requirements

The CMA has long advocated a high degree of transparency and member responsibility in the gathering and handling of consumers' personal information as essential ingredients in obtaining and maintaining public trust and confidence in information-based marketing. In fact, the Association has had its own Privacy Code—compulsory for members—since 1993. This Privacy Code forms an integral part of the Association's wider Code of Ethics and Standards of Practice.

Thus, with the introduction of a new national legal standard for the protection of personal information, CMA members should find themselves well prepared for the new framework, most of which presents technical and management changes to current industry-standard practices for information gathering and handling.

One significant aspect of the law, emphasized throughout its 10 principles, is the need for active management of marketers' information handling practices. This includes communicating with staff, and training staff in proper handling procedures for personal information and the importance of safeguarding personal information resources properly.

To ensure compliance with the law, it is important to read this document carefully and to consider how it will affect your organization.

Members are also reminded that five elements of CMA's Privacy Code containing provisions beyond those included in the legislation remain compulsory. These elements are addressed prior to discussion of the privacy law (see page 6).

## How to Use this Document

For ease of use this document provides the operative parts of the legislation (described formally as Schedule 1 of the Act, but excludes the portions dealing with electronic commerce, e-signatures and the Canadian Evidence Act) section-by-section in the left-hand column, with CMA commentary and any recommended member actions in the right-hand column. Where supplied for comparison, references to the CMA's Code of Ethics and Standards of Practice are incorporated verbatim and presented in italics in the right-hand column, using the same citations employed in the Code of Ethics and Standards of Practice (CESP), CESP at X.x.

**Please recognize that this document does not offer legal advice—it presents commentary on the government's intentions with the Act and expectations for administration and enforcement of the Act. Please consult with your own legal advisors for advice on steps your organization may need to take to ensure compliance with the Act and regulations.**

***January 2004***

# The Basic Principles

### 1. Accountability
An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.

### 2. Identifying Purposes
The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.

### 3. Consent
The knowledge and consent of the individual are required for the collection, use or disclosure of personal information, except where inappropriate.

### 4. Limiting Collection
The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

### 5. Limiting Use, Disclosure and Retention
Personal information shall not 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. Personal information shall be retained only as long as necessary for the fulfillment of those purposes.

### 6. Accuracy
Personal information shall be as accurate, complete and up-to-date as is necessary for the purposes for which it is to be used.

### 7. Safeguards
Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

### 8. Openness
An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

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

### 10. Challenging Compliance
An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.

## Additional privacy requirements for CMA members:

1. The CMA mandates that the meaningful opportunity for consumers to decline further marketing use of their name or other information must be repeated once every three years, at a minimum.

2. All CMA members must use the Do Not Contact service of the Association in their customer acquisition activities.

3. CMA members are obliged to provide consumers with the source of their name, upon request.

4. CMA member companies are strongly encouraged to adopt a list rental policy which restricts rental of information to companies which agree to comply with the CMA's Privacy Code.

5. By January 1, 2004, CMA members must offer existing or current customers an opportunity to opt-out of future marketing offers or solicitations that are unrelated to the original purchase. All opt-out opportunities must be easy to understand, easy to see and easy to execute.

# Canadian Privacy Legislation
# Commentary and Implementation Guidelines

## Principle 1 - Accountability

### 4.1 Principle 1 - Accountability

An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.

**CMA Commentary**

A re-statement of CMA's CESP at I7.2

*I 7.2 All CMA members must designate a staff manager to be responsible for adherence to the Principles of the Privacy Code.*

### 4.1.1

Accountability for the organization's compliance with the principles rests with the designated individual(s), even though other individuals within the organization may be responsible for the day-to-day collection and processing of personal information. In addition, other individuals within the organization may be delegated to act on behalf of the designated individual(s).

**CMA Commentary**

No change required to current CMA member practice. See CESP at I7.2.

*I 7.2 All CMA members must designate a staff manager to be responsible for adherence to the Principles of the Privacy Code.*

### 4.1.2

The identity of the individual(s) designated by the organization to oversee the organization's compliance with the principles shall be made known upon request.

**CMA Commentary**

Note the new obligation to make the privacy manager's name freely available, upon request—expands CESP at I7.2.

*I 7.2 All CMA members must designate a staff manager to be responsible for adherence to the Principles of the Privacy Code.*

**4.1.3**
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 a third party.

## CMA Commentary

The new legislation specifically places the onus to maintain control of the security of the information, even while it is in a third party's hands, such as for processing. See CESP at I5 and I6.

Accordingly, an important new practice will be to ensure—typically by contractual means—that any other party to which your organization passes personal information agrees to abide by the provisions of the federal law, and to assume the responsibility for doing so.

*I 5 Safely Storing Information About Consumers*

*All those involved in the transfer, rental, sale or exchange of mailing lists must be responsible for the protection of list data and should take appropriate measures to ensure against unauthorized access, alteration or dissemination of list data. Those who have access to such data should agree in advance to use such data only in an authorized manner.*

*I 6 Respecting Confidential and Sensitive Information*

*All list owners and users must be protective of the consumer's right to privacy and sensitive to the information collected on lists and subsequently considered for use, transfer, rental or sale.*

*Where a use of personal information that a reasonable person would consider to be sensitive and confidential has not been identified to the individual at the time of collection, then positive consent must be obtained prior to such further use of the personal information.*

*The industry recognizes that private personal data such as medical, financial and credit data must be protected by sectoral regulatory codes.*

### 4.1.4

Organizations shall implement policies and practices to give effect to the principles, including:

(a) implementing procedures to protect personal information;

(b) establishing procedures to receive and respond to complaints and inquiries;

(c) training staff and communicating to staff information about the organization's policies and practices; and

(d) developing information to explain the organization's policies and procedures.

### CMA Commentary

The new law requires marketers to be open and formal about their information-gathering and information-handling practices, and to establish and maintain company procedures covering information-handling.

Marketers should also note the staff training and communication requirements.

# Principle 2 - Identifying Purposes

## 4.2 Principle 2 - Identifying Purposes

The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.

### CMA Commentary

This section reflects CMA's CESP at I4.

*I 4 Controlling the Use of Information by Third Parties*

*The purposes for which information is collected shall be identified by the organization at or before the time the information is collected.*

*The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization.*

*All those involved in the transfer, rental, sale or exchange of mailing lists must establish and agree upon the exact nature of the list's intended usage prior to permission being given to use the list or to transfer the information.*

### 4.2.1
The organization shall document the purposes for which personal information is collected in order to comply with the Openness principle (Clause 4.8) and the Individual Access principle (Clause 4.9).

## CMA Commentary
This is a requirement for marketers to formalize their information-gathering needs, prior to collection of individuals' personal information.

### 4.2.2
Identifying the purposes for which personal information is collected at or before the time of collection allows organizations to determine the information they need to collect to fulfil these purposes. The Limiting Collection principle (Clause 4.4) requires an organization to collect only that information necessary for the purposes that have been identified.

## CMA Commentary
This section reflects CMA's requirement to limit the collection of personal information to that needed to fulfil identified purposes. See CESP at I4.

*I 4 Controlling the Use of Information by Third Parties*

*The purposes for which information is collected shall be identified by the organization at or before the time the information is collected.*

*The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization.*

*All those involved in the transfer, rental, sale or exchange of mailing lists must establish and agree upon the exact nature of the list's intended usage prior to permission being given to use the list or to transfer the information*

### 4.2.3

The identified purposes should be specified at or before the time of collection to the individual from whom the personal 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.

## CMA Commentary

This point addresses the collection personal information.

In many information-based marketing interactions, both the act of collecting personal information and the individual's consent to it are implicit. Such interactions include the use of paper-based forms and Web sites employing 'check boxes,' as well as consumer response to offers delivered by television or radio.

**Examples:** Completing and signing an insurance application form addresses both the collection and the individual's consent. Where the prospective collection of personal information may not be transparent to the individual—in electronic media, including the Internet, computer-based information services, electronic kiosks and databases—CMA members are currently obliged to notify consumers of the collection of information that could identify them personally (and which will be linked with clickstream data) prior to its collection and to provide a meaningful opportunity to decline collection or transfer of that information. (See CESP at E4.5)

*E4.5 Disclosure: When gathering data from individual consumers that could identify the consumer, and which will be linked with "clickstream" data, marketers shall advise consumers: a) what information is being collected; and, b) how the information will be used. The marketer shall provide access to this advisory before consumers submit data that could identify them.*

### 4.2.4

When personal information that has been collected is to be used for a purpose not previously identified, the new purpose shall be identified prior to use. Unless the new purpose is required by law, the consent of the individual is required before information can be used for that purpose. For an elaboration on consent, please refer to the Consent principle (Clause 4.3).

## CMA Commentary

Personal information collected for a marketing purpose would not require 'new consent' prior to another (new) marketing use. Marketers have the implied consent of current customers to continue to present offers.

As an illustration of a situation requiring 'new' consent: personal information collected for medical purposes being considered for a marketing purpose would require 'new' prior consent by the individual. In addition, as such information could also be considered 'sensitive' (CESP at I6), the type of consent required would be 'positive'.

*I 6 Respecting Confidential and Sensitive Information*

*All list owners and users must be protective of the consumer's right to privacy and sensitive to the information collected on lists and subsequently considered for use, transfer, rental or sale.*

*Where a use of personal information that a reasonable person would consider to be sensitive and confidential has not been identified to the individual at the time of collection, then positive consent must be obtained prior to such further use of the personal information.*

*The industry recognizes that private personal data such as medical, financial and credit data must be protected by sectoral regulatory codes.*

### 4.2.5
Persons collecting personal information should be able to explain to individuals the purposes for which the information is being collected.

#### CMA Commentary
CMA members already observe this requirement as a matter of sound business practice.

### 4.2.6
This principle is linked closely to the Limiting Collection principle (Clause 4.4) and the Limiting Use, Disclosure, and Retention principle (Clause 4.5).

#### CMA Commentary
No comment.

## Principle 3 - Consent

### 4.3 Principle 3 - Consent
The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.

#### CMA Commentary
This section recognizes that different types or forms of consent are appropriate to different types of information and their intended uses, and it reflects CMA members' use of:

(a) Express consent for the collection and use of personal information typically considered sensitive (financial, credit, medical or health), as well as for any new use (see CESP at I6);
(b) Negative option for the proposed transfer of non-sensitive personal information—meaningful opportunity to decline further marketing use or transfer must be presented before transfer and must be repeated at least once every three years (CESP at I1.1 and I1.2); and,
(c) Implied consent for maintenance of established relationships.

See also the commentary for 4.3.6.

In addition, the law recognizes that in certain circumstances personal information can be collected, used, or disclosed without the knowledge and consent of the individual. For example, legal, medical, or security reasons may make it impossible or impractical to seek consent. When information is being collected for the detection and prevention of fraud or for law enforcement, seeking the consent of the individual might defeat the purpose of collecting the information. Seeking consent may be impossible or inappropriate when the individual is a minor, seriously ill, or mentally incapacitated. In addition,

## 4.3 Principle 3 - Consent continued

organizations that do not have a direct relationship with the individual may not always be able to seek consent. For example, seeking consent may be impractical for a charity or a information-based marketing firm that wishes to acquire a mailing list from another organization. In such cases, the organization providing the list must have obtained consent before dislcosing personal information and anyone renting a list must ensure that this has been done.

*I 6: Respecting Confidential and Sensitive Information*

*All list owners and users must be protective of the consumer's right to privacy and sensitive to the information collected on lists and subsequently considered for use, transfer, rental or sale.*

*Where a use of personal information that a reasonable person would consider to be sensitive and confidential has not been identified to the individual at the time of collection, then positive consent must be obtained prior to such further use of the personal information.*

*The industry recognizes that private personal data such as medical, financial and credit data must be protected by sectoral regulatory codes.*

*I 1.1, I 1.2: Giving Consumers Control of How Information About Them is Used*

*1.1 Consumers must be provided with a meaningful opportunity to decline to have their name or other information used for any further marketing purposes by a third party.*

*1.3 This opportunity must be provided to the consumer before any information is transferred and must be repeated once every three years, at a minimum.*

### 4.3.1

Consent is required for the collection of personal information and the subsequent use or disclosure of this information. Typically, an organization will seek consent for the use or disclosure of the information at the time of collection. In certain circumstances, consent with respect to use or disclosure may be sought after the information has been collected but before use (for example, when an organization wants to use information for a purpose not previously identified).

### CMA Commentary

This clause expands on <u>when</u> consent may be obtained.

**Example:** Marketers' customer-acquisition efforts may include the collection of personal information in connection with other forms of communication, such as responding to a consumer's request for product or service information.

### 4.3.2
The principle requires "knowledge and consent". Organizations shall make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used. To make the consent meaningful, the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed.

### CMA Commentary
The requirement for "knowledge and consent" places an onus on marketers to make a reasonable effort to ensure the consumer understands that personal information is being collected and how it may be used. See CMA Commentary attached to Principle 4.2.3.

Accordingly the use of 'surveys' and similar information-gathering techniques must have bona fide purposes if used to obtain personal information. (See also Principle 4.4.2.)

### 4.3.3
An organization shall 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 the explicitly specified, and legitimate purposes.

### CMA Commentary
This section provides a prohibition of unreasonable demands for the supply of personal information. For example, it would be reasonable to require a new customer seeking to rent a video to provide personal information (such as home address—obtained from a driver's license or credit card) as security against the return of the video. It would not be reasonable to demand banking or mortgage information for the same security.

### 4.3.4
The form of the consent sought by the organization may vary, depending upon the circumstances and the type of information. In determining the form of consent to use, organizations shall take into account the sensitivity of the information. Although some information (for example, medical records and income records) is almost always considered to be sensitive, any information can be sensitive, depending on the context. For example, the names and addresses of subscribers to a newsmagazine would generally not be considered sensitive information. However, the names and addresses of subscribers to some special-interest magazines might be considered sensitive.

### CMA Commentary
This section introduces the concept that 'context' is also an important factor in determining the sensitivity of personal information, in addition to consideration of the type of information itself.

## 4.3.5

In obtaining consent, the reasonable expectations of the individual are also relevant. For example, an individual buying a subscription 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 can assume that the individual's request constitutes consent for specific purposes. On the other hand, an individual would not reasonably expect that personal information given to a health-care professional would be given to a company selling health-care products, unless consent were obtained. Consent shall not be obtained through deception.

## CMA Commentary

This section advances the new notion that the 'reasonable expectations' of the individual are relevant in determining the degree of sensitivity attached to personal information to be collected.

## 4.3.6

The way in which an organization seeks consent may vary, depending on the circumstances and the type of information collected. An organization should generally seek express consent when the information is likely to be considered sensitive. Implied consent would generally be appropriate when the information is less sensitive. Consent can also be given by an authorized representative (such as a legal guardian or a person having power of attorney).

## CMA Commentary

See also the commentary at Principle 4.3 regarding CMA members' use of three forms of consent, applicable to the collection, use or transfer of information of varying degrees of sensitivity.

**Example:** A catalogue marketer or magazine publisher has the recipients' implied consent to send further catalogues or solicit subscription renewals.

## 4.3.7

Individuals can give consent in many ways. For example:

(a) an application form may be used to seek consent, collect information, and inform the individual of the use that will be made of the information. By completing and signing the form, the individual is giving consent to the collection and the specified uses;

(b) a checkoff box may be used to allow individuals to request that their names and addresses not be given to other organizations. Individuals who do not check the box are assumed to consent to the transfer of this 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.

### CMA Commentary

This section illustrates how consent may be obtained in various media and relating to varying degrees of the sensitivity of the personal information to be collected.

See also the CMA commentary at Principle 4.3.

## 4.3.8

An individual may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. The organization shall inform the individual of the implications of such withdrawal.

### CMA Commentary

The obligation to advise the consumer of the consequences of his or her withdrawal of consent is new, however CMA members recognize that this is also sound business practice. (See CESP at I 1.4)

**Example:** Marketers may advise consumers withdrawing consent of 'what they won't receive' as a consequence of their choice.

*I 1.4 Giving consumers Control of How Information About Them is Used*
*In addition to the above, the marketer must remove the consumer's name from all internal marketing lists or lists for rental to a third party at the request of the consumer at any time, i.e., all member companies of CMA must maintain internal suppression lists for all media employed by the marketer.*

# Principle 4 - Limiting Collection

## 4.4 Principle 4 - Limiting Collection

The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

### CMA Commentary

This section reflects current CMA member practice in the limitation on personal information to be collected, per CESP at I 4.

*I 4 Controlling the Use of Information by Third Parties*
*The purposes for which information is collected shall be identified by the organization at or before the time the information is collected.*

*The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization.*

*All those involved in the transfer, rental, sale or exchange of mailing lists must establish and agree upon the exact nature of the list's intended usage prior to permission being given to use the list or to transfer the information.*

## 4.4.1

Organizations shall not collect personal information indiscriminately. Both the amount and the type of information collected shall be limited to that which is necessary to fulfil the purposes identified. Organizations shall specify the type of information collected as part of their information-handling policies and practices, in accordance with the Openness principle (Clause 4.8).

### CMA Commentary

This section reflects the CMA's limits on the collection of personal information (CESP at I 4), with the added specificity of limiting by both type and amount of information to be collected. See also the commentary and discussion, below, re Principle 4.6 (4.6.1-4.6.3) Accuracy of Information.

*I 4 Controlling the Use of Information by Third Parties*
*The purposes for which information is collected shall be identified by the organization at or before the time the information is collected.*

*The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization.*

*All those involved in the transfer, rental, sale or exchange of mailing lists must establish and agree upon the exact nature of the list's intended usage prior to permission being given to use the list or to transfer the information.*

### 4.4.2
The requirement that personal information be collected by fair and lawful means is intended to prevent organizations from collecting information by misleading or deceiving individuals about the purpose for which information is being collected. This requirement implies that consent with respect to collection must not be obtained through deception.

### CMA Commentary
This section includes a specific prohibition against marketing techniques that obtain personal information under false pretences. For example, the use of a 'survey' pretext where there is no bona fide information-gathering purpose, is prohibited. (See also Principle 4.3.2 for a different perspective on the same issue.)

### 4.4.3
This principle is linked closely to the Identifying Purposes principle (Clause 4.2) and the Consent principle (Clause 4.3).

### CMA Commentary
No comment.

## Principle 5 - Limiting Use, Disclosure, and Retention

### 4.5 Principle 5 - Limiting Use, Disclosure, and Retention
Personal information shall not 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. Personal information shall be retained only as long as necessary for the fulfilment of those purposes.

### CMA Commentary
While the CMA has recognized the appropriateness of limiting the amount of personal information collected to that required to meet a defined purpose (CESP at I 4), this section introduces the notion that personal information should not be retained after it has served its defined purpose.

*I 4 Controlling the Use of Information by Third Parties*
*The purposes for which information is collected shall be identified by the organization at or before the time the information is collected.*

*The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization.*

*All those involved in the transfer, rental, sale or exchange of mailing lists must establish and agree upon the exact nature of the list's intended usage prior to permission being given to use the list or to transfer the information.*

### 4.5.1
Organizations using personal information for a new purpose shall document this purpose (see Clause 4.2.1).

### CMA Commentary
A further reiteration of the need for more formal information-handling policies and practices, as described at Principle 4.1.4.

### 4.5.2
Organizations should develop guidelines and implement procedures with respect to the retention of personal information. These guidelines should include minimum and maximum retention periods. Personal information that has been used to make a decision about an individual shall be retained long enough to allow the individual access to the information after the decision has been made. An organization may be subject to legislative requirements with respect to retention periods.

### CMA Commentary
This section introduces the new concept that marketers should not retain personal information indefinitely, or beyond meeting the specific needs for which it was collected.

**Member action:** Members should develop guidelines and implement procedures to direct the retention of personal information as part of their overall personal information-handling procedures. (See Principle 4.1.4.) In addition, members are reminded that there are often regulatory requirements governing the retention of business information.

### 4.5.3
Personal information that is no longer required to fulfil the identified purposes should be destroyed, erased, or made anonymous. Organizations shall develop guidelines and implement procedures to govern the destruction of personal information.

### CMA Commentary
This section introduces the new concept that extends marketers' responsibility for the safe handling of personal information through its destruction and/or disposal.

**Member action:** CMA members should develop formal guidelines and implement procedures to ensure the safe destruction or disposal of personal information no longer required.

### 4.5.4
This principle is closely linked to the Consent principle (Clause 4.3), the Identifying Purposes principle (Clause 4.2), and the Individual Access principle (Clause 4.9).

### CMA Commentary
No comment.

# Principle 6 - Accuracy

## 4.6 Principle 6 - Accuracy

Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.

### CMA Commentary

See commentary for following Principles 4.6.1. - 4.6.3.

## 4.6.1

The extent to which personal information shall be accurate, complete, and up-to-date will depend upon the use of the information, taking into account the interests of the individual. Information shall be sufficiently accurate, complete, and up-to-date to minimize the possibility that inappropriate information may be used to make a decision about the individual.

### CMA Commentary

This section elaborates current CMA member practices, including the limitations on collecting information only for documented purposes. See CESP at I 4, and the following two Principles (4.6.2 and 4.6.3).

*I 4 Controlling the Use of Information by Third Parties*
*The purposes for which information is collected shall be identified by the organization at or before the time the information is collected.*

*The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization.*

*All those involved in the transfer, rental, sale or exchange of mailing lists must establish and agree upon the exact nature of the list's intended usage prior to permission being given to use the list or to transfer the information.*

## 4.6.2

An organization shall not routinely update personal information, unless such a process is necessary to fulfil the purposes for which the information was collected.

### CMA Commentary

This Principle (4.6.2) should be read and considered alongside the following Principle (4.6.3). Taken together, they oblige marketers to keep personal information on consumers as up-to-date as appropriate for the defined need, but no more so.

## 4.6.3

Personal information that is used on an ongoing basis, including information that is disclosed to third parties, should generally be accurate and up-to-date, unless limits to the requirement for accuracy are clearly set out.

### CMA Commentary

This Principle (4.6.3.) complements the previous Principle (4.6.2.)

# Principle 7 - Safeguards

## 4.7 Principle 7 - Safeguards

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

### CMA Commentary

No comment. (See CESP at I 5)

*I 5 Safely Storing Information About Consumers*

*All those involved in the transfer, rental, sale or exchange of mailing lists must be responsible for the protection of list data and should take appropriate measures to ensure against unauthorized access, alteration or dissemination of list data. Those who have access to such data should agree in advance to use such data only in an authorized manner.*

## 4.7.1

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

### CMA Commentary

No comment. (See CESP at I 5)

*I 5 Safely Storing Information About Consumers*

*All those involved in the transfer, rental, sale or exchange of mailing lists must be responsible for the protection of list data and should take appropriate measures to ensure against unauthorized access, alteration or dissemination of list data. Those who have access to such data should agree in advance to use such data only in an authorized manner.*

## 4.7.2

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. The concept of sensitivity is discussed in Clause 4.3.4.

### CMA Commentary

This Principle introduces the concept of different degrees of protection to be afforded to different types (different degrees of the sensitivity) of information.

### 4.7.3
The methods of protection should include

(a) physical measures, for example, locked filing cabinets and restricted access to offices;

(b) organizational measures, for example, security clearances and limiting access on a "need-to-know" basis; and,

(c) technological measures, for example, the use of passwords and encryption.

### CMA Commentary
This Principle describes different types of protection to be afforded sensitive personal information in marketers' custody.

Marketers should ensure that the personal information in their custody is well protected according to these measures.

### 4.7.4
Organizations shall make their employees aware of the importance of maintaining the confidentiality of personal information.

### CMA Commentary
This is an administrative issue, directing marketers to ensure the confidentiality of personal information held by their organizations.

### 4.7.5
Care shall be used in the disposal or destruction of personal information, to prevent unauthorized parties from gaining access to the information (see Clause 4.5.3).

### CMA Commentary
This Principle is a recapitulation of Principle 4.5.3., with the added specificity of 'unauthorized parties' (presumably inside or outside the marketer's organization); 'gaining access' may include physical possession of personal information assets, as well as the ability to understand the personal information contained in such assets.

## Principle 8 - Openness

### 4.8 Principle 8 - Openness
An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

### CMA Commentary
This is a new provision, requiring CMA members to be more forthcoming regarding their personal information handling practices.

## 4.8.1

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

## CMA Commentary

This is a recapitulation of the previous Principle, adding the notion that marketers should make information about their personal information handling practices and procedures easy to understand by consumers. (See CESP at I 2.1 and 2.2)

*I 2.1 & 2.2: Providing Consumers with the Right of Access to Information*

*2.1 The industry endorses the right of the consumer to know the source of his/her name used in any information-based marketing program.*

*Marketers must make all reasonable efforts to provide this information to the consumer on request.*

*2.2 Additionally, consumers have the right to know what information is held in their customer files and the right to question and request correction of any erroneous information.*

*Marketers must make all reasonable efforts to provide this information to the consumer on request. In the case of disputes between consumers and marketers, CMA will act as mediator and may require that marketers adjust data or annotate customer files.*

## 4.8.2

The information made available shall include

(a) the name or title, and the address, of the person who is accountable for the organization's policies and practices 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).

## CMA Commentary

This Principle provides a catalogue of personal information handling policies and procedures marketers should be prepared to explain to consumers.

This enriches the CMA's CESP at I 2:

*I 2.1 & 2.2: Providing Consumers with the Right of Access to Information*

*2.1 The industry endorses the right of the consumer to know the source of his/her name used in any information-based marketing program.*

*Marketers must make all reasonable efforts to provide this information to the consumer on request.*

*2.2 Additionally, consumers have the right to know what information is held in their customer files and the right to question and request correction of any erroneous information.*

*Marketers must make all reasonable efforts to provide this information to the consumer on request. In the case of disputes between consumers and marketers, CMA will act as mediator and may require that marketers adjust data or annotate customer files.*

### 4.8.3
An organization may make information on its policies and practices available in a variety of ways. The method chosen depends on the nature of its business and other considerations. For example, an organization may choose to make brochures available in its place of business, mail information to its customers, provide online access, or establish a toll-free telephone number.

### CMA Commentary
This is a summary description of the different ways marketers may choose to communicate their information handling policies and procedures to consumers, with the thought that marketers may choose a medium of communication suited to their businesses.

## Principle 9 - Individual Access

### 4.9 Principle 9 - Individual Access
Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

### CMA Commentary
This is a statement of the right of consumers to know if a marketer holds personal information about them—per CESP at I 2.1 and I 2.2.

See also the commentary at 4.9.3.

The law also provides exceptions to this requirement, which enable marketers to decline to provide access to a consumer's personal information on grounds of prohibitive cost, reference to other persons, proprietary commercial sensitivity, solicitor-client privilege, or other legal or security reasons.

*I 2.1 & 2.2 Providing Consumers with the Right of Access to Information*

*2.1 The industry endorses the right of the consumer to know the source of his/her name used in any information-based marketing program.*

*Marketers must make all reasonable efforts to provide this information to the consumer on request.*

*2.2 Additionally, consumers have the right to know what information is held in their customer files and the right to question and request correction of any erroneous information.*

*Marketers must make all reasonable efforts to provide this information to the consumer on request. In the case of disputes between consumers and marketers, CMA will act as mediator and may require that marketers adjust data or annotate customer files.*

### 4.9.1

Upon request, an organization shall inform an individual whether or not the organization holds personal information about the individual. Organizations are encouraged to indicate the source of this information. The organization shall allow the individual access to this information. However, the organization may choose to make sensitive medical information available through a medical practitioner. In addition, the organization shall provide an account of the use that has been made or is being made of this information and an account of the third parties to which it has been disclosed.

## CMA Commentary

This is a statement of the right of consumers to know if a marketer holds personal information about them—per CESP at I 2.1 and I 2.2. re source of name.

See the commentary below, re 4.9.3., which notes that marketers are not obliged to detail their use of personal information when doing so would conflict with commercial proprietary concerns.

*I 2.1 & 2.2: Providing Consumers with the Right of Access to Information*

*2.1 The industry endorses the right of the consumer to know the source of his/her name used in any information-based marketing program.*

*Marketers must make all reasonable efforts to provide this information to the consumer on request.*

*2.2 Additionally, consumers have the right to know what information is held in their customer files and the right to question and request correction of any erroneous information.*

*Marketers must make all reasonable efforts to provide this information to the consumer on request. In the case of disputes between consumers and marketers, CMA will act as mediator and may require that marketers adjust data or annotate customer files.*

### 4.9.2

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. The information provided shall only be used for this purpose.

## CMA Commentary

This is a requirement for consumers to provide marketers with sufficient personal information to determine whether they do hold a personal information file on that individual.

It is noteworthy that the provision of such personal information shall not be used for any other purpose.

## 4.9.3

In providing an account of third parties to which it has disclosed personal information about an individual, an organization should attempt to be as specific as possible. When it is not possible to provide a list of the organizations to which it has actually disclosed information about an individual, the organization shall provide a list of organizations to which it may have disclosed information about the individual.

### CMA Commentary

See commentary at Principle 4.9 for reference to specified exceptions to granting consumers access to personal information.

## 4.9.4

An organization shall respond to an individual's request within a reasonable time and at minimal or no cost to the individual. The requested information shall 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 shall be provided.

### CMA Commentary

The costs of re-creating a prospect personal information database used on a one-time basis may be significant. Accordingly, "minimal cost" may be the marketer's actual cost. The consumer should be advised of this cost and agreement obtained prior to undertaking the work.

## 4.9.5

When an individual successfully demonstrates the inaccuracy or incompleteness of personal information, the organization shall amend the information as required. Depending upon the nature of the information challenged, amendment involves the correction, deletion, or addition of information. Where appropriate, the amended information shall be transmitted to third parties having access to the information in question.

### CMA Commentary

This is a technical extension of the current 'right to question and request correction (including CMA mediation and mandated correction)' provided by CESP at I 2.2. This provision specifically grants individuals the right to have personal information corrected by the marketer holding it.

Here, the 'where appropriate' notation refers to the potential for negative consequences for the individual, such as a negative credit report.

*I 2.2 Providing Consumers with the Right of Access to Information*

*2.2 Additionally, consumers have the right to know what information is held in their customer files and the right to question and request correction of any erroneous information.*

*Marketers must make all reasonable efforts to provide this information to the consumer on request. In the case of disputes between consumers and marketers, CMA will act as mediator and may require that marketers adjust data or annotate customer files.*

### 4.9.6
When a challenge is not resolved to the satisfaction of the individual, the substance of the unresolved challenge shall be recorded by the organization. When appropriate, the existence of the unresolved challenge shall be transmitted to third parties having access to the information in question.

### CMA Commentary
Marketers are now required to note unresolved challenges to the accuracy of personal information and to share this information with third parties with which it has shared the personal information.

## Principle 10 - Challenging Compliance

### 4.10 Principle 10 - Challenging Compliance
An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.

### CMA Commentary
These new sections require marketers to establish formal inquiry and complaint handling mechanisms, and to make these mechanisms (and their operation) known to consumers who inquire or complain. See Principles 4.10.1 - 4.10.3, below.

### 4.10.1
The individual accountable for an organization's compliance is discussed in Clause 4.1.1.

### CMA Commentary
No comment.

### 4.10.2
Organizations shall put procedures in place to receive and respond to complaints or inquiries about their policies and practices relating to the handling of personal information. The complaint procedures should be easily accessible and simple to use.

### CMA Commentary
As discussed above re Principle 4.10.

### 4.10.3
Organizations shall inform individuals who make inquiries or lodge complaints of the existence of relevant complaint procedures. A range of these procedures may exist. For example, some regulatory bodies accept complaints about the personal-information handling practices of the companies they regulate.

### CMA Commentary
As discussed above re Principle 4.10.

### 4.10.4
An organization shall investigate all complaints. If a complaint is found to be justified, the organization shall take appropriate measures, including, if necessary, amending its policies and practices.

### CMA Commentary
This new requirement directs marketers to respond to inquiries and complaints from consumers, according to the marketer's established policies and procedures.

# Application and Enforcement of the Act

The new Act is to be applied by the Office of the Federal Privacy Commissioner, with a variety of means of enforcement, including court-ordered sanctions and fines. The application of the Act is currently under consultation between the CMA and the Federal Privacy Commissioner.

## Investigation of Complaints

Under the Act, individuals may file complaints with the Commissioner and, upon believing there are reasonable grounds, the Commissioner may undertake a process of investigation that includes:

- The ability to summon and enforce the appearance of persons and compel their oral or written evidence under oath;
- The ability to administer oaths;
- The ability to receive and accept evidence under oath, under affidavit, or otherwise, whether or not it is or would be admissible in a court;
- The ability to enter premises (other than a dwelling-house)—subject to a reasonable time and the satisfaction of the organization's security procedures;
- The ability to converse privately with any person and make inquiries within such premises; and,
- The ability to examine or obtain copies or extracts of records in such premises regarding any matter relevant to the investigation.

In addition, the Commissioner may attempt to resolve disputes through mediation or conciliation.

The Commissioner is generally required to report on complaints within one year.

Complainants may apply to the Court (the Federal Court of Canada) for a hearing on the Commissioner's report. The Commissioner may also apply to the Court for a hearing on behalf of a complainant, appear before the Court on behalf of a complainant and, with the leave of the Court, appear as a party at any hearing.

The Court may, in addition to any other remedies: issue an order for an organization to comply with the privacy law provisions; order an organization to publish a notice regarding correction of its practices; and, award damages, including damages for humiliation to the complainant.

## Audits

If the Commissioner has reasonable grounds to believe that an organization is contravening provisions of the privacy law, he may—on reasonable notice and at a reasonable time—conduct an audit of an organization's personal information management practices.

Under these terms, the Commissioner has the same broad discretion as described under Investigation of Complaints.

## Communication

The Commissioner has broad powers under the Act—and acting in the public interest—to publicize:

- information about an organization's information handling practices;
- information relating to an investigation or audit;
- prosecutions, hearings or appeals; and,
- The Commissioner may inform the Attorney General of Canada, or of a province or territory, information or evidence relating to the commission of an offence.

In these activities the Commissioner and his delegated representatives, acting in good faith, are immune from civil or criminal proceedings.

In addition, the Commissioner is required to conduct public information and education activities and research on the protection of personal privacy, and to report to Parliament annually on activities under the Act.

## Fines

Penalties under the Act for knowing contraventions, or for obstruction of the Commissioner or his delegate in the investigation of a complaint or conduct of an audit include fines of $10,000 upon summary conviction, or an indictable offence and liability to a fine of up to $100,000.

## For more information, visit these Web sites:

**Canadian Marketing Association:** www.the-cma.org

**House of Commons:** www.parl.gc.ca

**Office of the Federal Privacy Commissioner:** www.privcom.gc.ca

**Canadian Standards Association:** www.csa-international.org

## Notes