

Overview:

CMA Privacy Compliance Guide

CMA Members can access the full Guide [here](#).

A recognized leader in industry self-regulation, the Canadian Marketing Association has a Code of Ethics and Standards of Practice, and series of guides, that establish best practices for marketers in Canada and assist members with understanding and navigating regulatory frameworks.

Overview: CMA Privacy Compliance Guide

PURPOSE AND BACKGROUND

This guide contains information on implementing Canada's federal privacy law, the Personal Information Protection and Electronic Documents Act (PIPEDA), and the seven compulsory privacy requirements beyond those included in PIPEDA that are detailed in the Canadian Marketing Association's [Code of Ethics and Standards of Practice](#), "the Code". (see page 5)

This Guide is not intended to take the place of legal advice. Rather, it presents commentary on the intent and purpose of PIPEDA, and expectations for administration and enforcement of it. Please consult with your legal counsel for advice on steps your organization may need to take to ensure compliance with the Act and its regulations.

The CMA and its members recognize that maintaining high standards of practice is a fundamental responsibility to the public and the foundation for a successful and strong business community in Canada.

The CMA is the leader in providing legislative and regulatory guidelines and articulating best practices for the marketing profession in Canada. As the self-regulatory body for the marketing profession in Canada, we provide educational resources to maintain and strengthen the professionalism and integrity of the marketing community. Our Code of Ethics and Standards of Practice, which is widely recognized as a benchmark for effective self-regulation, is mandatory for members and regularly updated.

INTRODUCTION

In January 2004, PIPEDA came into effect across Canada, setting the rules for the collection, use and disclosure of personal information by Canadian organizations in the course of commercial activities.

The federal law, echoed by Section J1 of the Code, is based on the 10 basic principles of the Canadian Standards Association (CSA) Model Code for the Protection of Personal Information (see page 4).

PIPEDA is enforced by the Office of the Privacy Commissioner of Canada, also referred to as the "OPC" or the "Privacy Commissioner." The OPC, which is independent of government and reports directly to Parliament, can audit and investigate the personal information management practices of an organization on reasonable grounds and make nonbinding recommendations but cannot issue binding orders or fines unless ordered to do so by the Federal Court.

In June 2015, the [Digital Privacy Act](#) became law, amending PIPEDA to include new exemptions for consent, enhanced powers for the OPC, and more (see the updates [here](#)). In November 2018, [Breach of Security Safeguards Regulations](#) came into effect. In January 2019, new [Guidelines for Obtaining Meaningful Consent](#) came into effect.

Many jurisdictions around the world are reviewing and updating their privacy laws and Canada is no different. The CMA is actively involved in discussions with officials on legislative reform. Our submissions to government, along with other privacy resources, can be found [here](#).

How the Law Applies

PIPEDA applies to most private sector organizations across Canada in the course of commercial activities except in Québec, British Columbia and Alberta. These provinces have their own private sector laws that are deemed "substantially similar" to PIPEDA. PIPEDA also applies to [federally-regulated businesses](#) operating in Canada and their employee information, including in Québec, British Columbia, and Alberta. In addition, all businesses that operate in Canada and handle personal information that crosses provincial or national borders are subject to PIPEDA, regardless of which province or territory they are based in.

Please note non-profit status does not automatically exempt an organization from PIPEDA. Non-profit, charitable and membership-based organizations can still be engaged in commercial activity that triggers PIPEDA, such as the selling, bartering, or leasing of donor, membership or other fundraising lists. The court has held that PIPEDA has extraterritorial application (to organizations outside of Canada) if there is a "real and substantial connection" between Canada and the activity undertaken in a foreign jurisdiction.

Overview: CMA Privacy Compliance Guide

To find out which Canadian privacy law applies to your organization and its specific activities, see the OPC website [here](#). Other privacy laws may apply to your organization instead of or in addition to PIPEDA, for example, if your organization is a federal government institution subject to [the Privacy Act](#).

PIPEDA applies to the collection, use and disclosure of personal information by organizations in the course of commercial activities. "Personal information" means information about an identifiable individual which includes any factual or subjective information about that individual in any form, including, for example, their name, address, purchase habits, age, gender, opinions about the individual, income, physical description, existence of a dispute between a consumer and a merchant, education, employment, religious and political beliefs or affiliations, visual images or videotapes where individuals may be identified and more.

An important exclusion (see the full list [here](#)) includes an organization's collection, use or disclosure of business contact information solely for communicating with a person in relation to their employment, business or profession.

Regarding the limited exemption for business contact information (name, title, business address, telephone number or email of an employee of an organization), the CMA Code states the following:

Privacy and Business-to-Business (Code Section J2): Business-to-business marketing is exempt from PIPEDA and from the 10 Privacy Principles above when the collection, use or disclosure of contact information is limited to name, and/or title/position, and/or business address(es), and/or business phone number(s). If any other personal information is collected, used or disclosed then the provisions of PIPEDA and this section apply.

and:

Published Business Email Addresses (Code Section N4.2): Published business email addresses must only be used for marketing communications relevant to the business of the email recipient, provided a statement does not accompany the published address indicating that the address is not to be used for the purpose of marketing communications.

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.

Marketers are therefore advised that the prudent course of action is to assume that the law covers their operations and to ensure their organization complies with its requirements. Marketers should also take note of the requirements of CASL and how the two laws may interact. See the [CMA Guide to CASL](#).

The 10 Privacy Principles of PIPEDA and Section J1 of the Code

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 being 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.

Reasonable Person Concept: In addition to these principles, PIPEDA contains an overarching obligation that any collection, use or disclosure of personal information must only be for purposes that a reasonable person would consider as appropriate in the circumstances.

Seven Additional Privacy Requirements for CMA Members

- 1. Use of CMA Do Not Contact Service (Code Section J3)**

Marketers must use [CMA's Do Not Mail Service](#) when conducting a consumer mail campaign. The service must be used regardless of whether the campaign is being conducted in-house or through the use of an agency. This does not apply to B2B marketing, or to current customers, who can separately request that they be included on an organization's internal do not contact list. When conducting telephone and/or fax marketing campaigns, marketers must use the federal government's [National Do Not Call List](#) in accordance with the rules of that program.
- 2. Opt-Out Opportunity (Code Section J4)**

Recognizing that a consumer can opt-out of receiving marketing communications at any time, marketers must present consumers, including current customers, an easy-to-see, easy-to-understand and easy-to-execute opportunity to decline further marketing use of their name or other information at least once every three years. On all electronic marketing communications marketers must present consumers, including current customers, with the prescribed unsubscribe functionality to decline further marketing on every electronic communication in order to be compliant with Canada's Anti-Spam Law. See also Sections N3.10, N4.6 and N4.7 of this Code, Fax Marketing Opt-Out, Email Marketing Identification Requirements and Unsubscribe Opportunity and Text (SMS) Marketing Identification Requirements and Unsubscribe Requirements. For further information on Canada's Anti-Spam Law, members should consult the [CMA Guide to Canada's Anti-Spam Law](#).
- 3. Privacy Notice to Consumers (Code Section J5)**

A privacy notice to consumers is your organization's privacy commitment to its customers. It may also be known as a privacy policy. Marketers must clearly display a privacy notice across their digital platforms that articulates the organization's practices with respect to the collection, use and disclosure of the personal information of consumers. Access to the privacy policy must be provided in every location, site or page from which the marketer is collecting personal information. The [CMA Guide to Transparency for Consumers](#) outlines best practices to help organizations simplify their privacy notice and practices, and tailor them to their business model and consumers' preferences.
- 4. List Rental Practices (Code Section J6)**

Marketers must only rent or transfer their lists where they have a contractual guarantee that list users will abide by the relevant privacy and anti-spam laws in Canada. Further, marketers should adopt a list rental and data transfer policy that limits rental of information only to organizations that agree to comply with Section J3 of this Code, Use of [CMA Do Not Mail Service](#). (See also [CMA List and Data Transfer Guidelines](#) and [CMA Guide to Canada's Anti-Spam Law](#).)
- 5. Unlisted Numbers (Code Section N3.5)**

Marketers must not knowingly call any consumer or business who has an unlisted or unpublished telephone number, except where the telephone number was furnished by the consumer or business to that marketer, or by a third party with the consumer's consent.
- 6. Online Interest-based Advertising (Code Section N4.10)**

Online interest-based advertising, sometimes referred to as online behavioural advertising, refers to tracking consumers' online activities over time in order to deliver advertisements that are relevant to individuals' inferred interests. In advertising their goods or services through online interest-based advertising, marketers may directly or indirectly make use of service providers that include communications agencies, ad networks and website publishers.

PIPEDA and the Code apply to any personal information collected for internet and downloadable app interest-based advertising. Web browsing data may be considered personal information where that data can be connected to an identifiable individual. Without limiting the scope of these obligations, marketers should also be guided by the following principles when using internet and app interest-based advertising: (see also, [Section J](#) of this Code)

Overview: CMA Privacy Compliance Guide

- **Transparency:** Marketers using online interest-based advertising should ensure, by contract where necessary, that they, and the ad networks and website publishers used to display interest-based ads on their behalf, exercise transparency about the collection, use, disclosure and retention of data concerning consumers' online activities over time. Transparency means (a) openness and providing clear explanatory information about how browsing information is collected and what the information is used for and (b) an easy means to draw consumers' attention to that information; both in a manner consistent with accepted industry best practices (see also, the [Digital Advertising Alliance of Canada](#))
- **Consent:** Marketers must take the appropriate steps to ensure that the ad networks and online publishers that are used to display interest-based ads on their behalf offer consumers a clear and easy to see, easy to understand and easy to execute means to opt-out from having their online activities over time tracked to support the delivery of interest-based ads. Marketers using this type of advertising should ensure that they or their service providers use established industry best practices to provide notice of data collection, use, disclosure and retention for interest-based advertising, and that appropriate consent is being obtained from consumers. (see also, the [CMA Opt-out Consent Guidelines](#))
- **Children:** Marketers should not engage in or contract for the use of online interest-based advertising that is knowingly directed at, or knowingly conducted on, websites principally aimed at audiences of children under age 13, except in situations where express opt-in consent has been obtained separately from parent(s) or guardian(s). (See also, Section K of this code, [Marketing to Children](#))

7. Internal Do Not Mail List (Code Section N5.2)

At the request of a consumer or business, including a current customer, marketers must promptly add names and addresses to an internal do not contact list and cease marketing to that current customer, consumer or business at that address. Names and addresses must be retained on the internal do not contact list for three years.

Not for redistribution except with the express permission of the CMA. The [CMA Code of Ethics and Standards of Practice](#) and related [Compliance and Best Practices Guides](#) do not purport to replace legal advice or to provide legal guidance. Marketers should inform themselves about relevant laws that apply to them.

CMA would like to acknowledge and thank the members of the [Privacy and Data Advisory Committee](#) for their help in creating this Guide.

This Guide is current as of January 28, 2020.

© 2020 Canadian Marketing Association