

THE CGA MODEL PRIVACY CODE

The CGA Model Privacy Code (Privacy Code) has been made available to assist members of CGA (Members) to meet the obligations of new federal privacy legislation, which regulates the collection, use and disclosure of personal information in commercial activities.

The Privacy Code is intended to serve as a template for Members' customization. The entire Privacy Code should be fully reviewed by legal counsel with expertise in privacy law before Members rely or make use of it in relation to their specific situation. Sections of the Privacy Code that require particular attention have been noted in square brackets for your review and customization.

The Privacy Code and other privacy compliance tools made available by CGA do not constitute legal advice. 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 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 Members' use of the Privacy Code and/or other privacy compliance tools made available by CGA.

THE [INSERT NAME OF ORGANIZATION] PRIVACY CODE

Table of Contents

Introduction

Summary of Principles

Scope and Application

Definitions

The [INSERT NAME OF ORGANIZATION] Privacy Code in Detail

Principle 1 - Accountability

Principle 2 - Identifying Purposes for Collection of Personal Information

Principle 3 - Obtaining Consent for Collection, Use or Disclosure of Personal Information

Principle 4 - Limiting Collection of Personal Information

Principle 5 - Limiting Use, Disclosure, and Retention of Personal Information

Principle 6 - Accuracy of Personal Information

Principle 7 - Security Safeguards

Principle 8 - Openness Concerning Policies and Procedures

Principle 9 - [CLIENT/CUSTOMER] and Employee Access to Personal Information

Principle 10 - Challenging Compliance

Additional Information

Introduction

At [INSERT NAME OF ORGANIZATION], respecting privacy is an important part of our commitment to our [CLIENTS/CUSTOMERS] and employees. That is why we have developed The [INSERT NAME OF ORGANIZATION] Privacy Code. The [INSERT NAME OF ORGANIZATION] Privacy Code is a statement of principles and guidelines regarding the minimum requirements for the protection of personal information provided by [INSERT NAME OF ORGANIZATION] to its [CLIENTS/CUSTOMERS] and employees. The objective of The [INSERT NAME OF ORGANIZATION] Privacy Code is to promote responsible and transparent personal information management practices in a manner consistent with the provisions of the *Personal Information Protection and Electronic Documents Act* (Canada).

[INSERT NAME OF ORGANIZATION] will continue to review The [INSERT NAME OF ORGANIZATION] Privacy Code to make sure that it is relevant and remains current with changing industry standards, technologies and laws.

Summary of Principles

Principle 1 - Accountability

[INSERT NAME OF ORGANIZATION] is responsible for personal information under its control and shall designate one or more persons who are accountable for [INSERT NAME OF ORGANIZATION]'s compliance with the following principles.

Principle 2 - Identifying Purposes for Collection of Personal Information

[INSERT NAME OF ORGANIZATION] shall identify the purposes for which personal information is collected at or before the time the information is collected.

Principle 3 - Obtaining Consent for Collection, Use or Disclosure of Personal Information

The knowledge and consent of a [CLIENT/CUSTOMER] or employee are required for the collection, use, or disclosure of personal information, except where inappropriate.

Principle 4 - Limiting Collection of Personal Information

[INSERT NAME OF ORGANIZATION] shall limit the collection of personal information to that which is necessary for the purposes identified by [INSERT NAME OF ORGANIZATION]. [INSERT NAME OF ORGANIZATION] shall collect personal information by fair and lawful means.

Principle 5 - Limiting Use, Disclosure, and Retention of Personal Information

[INSERT NAME OF ORGANIZATION] shall not use or disclose personal information for purposes other than those for which it was collected, except with the consent of the individual or as required by law.

Principle 6 - Accuracy of Personal Information

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

Principle 7 - Security Safeguards

[INSERT NAME OF ORGANIZATION] shall protect personal information by security safeguards appropriate to the sensitivity of the information.

Principle 8 - Openness Concerning Policies and Procedures

[INSERT NAME OF ORGANIZATION] shall make readily available to [CLIENTS/CUSTOMERS] and employees specific information about its policies and procedures relating to the management of personal information.

Principle 9 – [CLIENT/CUSTOMER] and Employee Access to Personal Information

[INSERT NAME OF ORGANIZATION] shall inform a [CLIENT/CUSTOMER] or employee of the existence, use, and disclosure of his or her personal information upon request and shall give the individual access to that information. A [CLIENT/CUSTOMER] or employee shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

Principle 10 - Challenging Compliance

A [CLIENT/CUSTOMER] or employee shall be able to address a challenge concerning compliance with the above principles to the designated person or persons accountable for [INSERT NAME OF ORGANIZATION]'s compliance with The [INSERT NAME OF ORGANIZATION] Privacy Code.

Scope and Application

The ten principles that form the basis of The [INSERT NAME OF ORGANIZATION] Privacy Code are interrelated and [INSERT NAME OF ORGANIZATION] shall adhere to the ten principles as a whole. Each principle must be read in conjunction with the accompanying commentary. As permitted by the *Personal Information Protection and Electronic Documents Act* (Canada), the commentary in The [INSERT NAME OF ORGANIZATION] Privacy Code has been drafted to reflect personal information issues specific to [INSERT NAME OF ORGANIZATION].

The scope and application of The [INSERT NAME OF ORGANIZATION] Privacy Code are as follows:

- The [INSERT NAME OF ORGANIZATION] Privacy Code applies to personal information collected, used, or disclosed by [INSERT NAME OF ORGANIZATION] in the course of commercial activities.
- The [INSERT NAME OF ORGANIZATION] Privacy Code applies to the management of personal information in any form, whether oral, electronic or written.
- The [INSERT NAME OF ORGANIZATION] Privacy Code does not impose any limits on the collection, use or disclosure of the following information by [INSERT NAME OF ORGANIZATION]:
 - (a) an employee's name, title or business address or telephone number;
 - (b) information that [INSERT NAME OF ORGANIZATION] collects, uses or discloses for journalistic, artistic or literary purposes and does not collect, use or disclose for any other purpose; or
 - (c) other information about the individual that is publicly available and is specified by regulation pursuant to the *Personal Information Protection and Electronic Documents Act* (Canada).
- The [INSERT NAME OF ORGANIZATION] Privacy Code will not typically apply to information regarding [INSERT NAME OF ORGANIZATION]'s corporate [CLIENTS/CUSTOMERS]. However, such information may be protected by other [INSERT NAME OF ORGANIZATION] policies and practices and through contractual arrangements.
- The application of The [INSERT NAME OF ORGANIZATION] Privacy Code is subject to the requirements and provisions of the *Personal Information Protection and Electronic Documents Act* (Canada), the regulations enacted thereunder, and any other applicable legislation or regulation.

Definitions

collection: The act of gathering, acquiring, recording, or obtaining personal information from any source, including third parties, by any means.

consent: Voluntary agreement for the collection, use and disclosure of personal information for defined purposes. Consent can be either express or implied and can be provided directly by the individual or by an authorized representative. Express consent can be given orally, electronically or in writing, but is always unequivocal and does not require any inference on the part of [INSERT NAME OF ORGANIZATION]. Implied consent is consent that can reasonably be inferred from an individual's action or inaction.

[CLIENT/CUSTOMER]: An individual who purchases or otherwise acquires or uses any of [INSERT NAME OF ORGANIZATION]'s products or services or otherwise provides personal information to [INSERT NAME OF ORGANIZATION] in the course of [INSERT NAME OF ORGANIZATION]'s commercial activities.

disclosure: Making personal information available to a third party.

employee: An employee of or independent contractor to [INSERT NAME OF ORGANIZATION].

personal information: Information about an identifiable individual, but does not include the name, title, business address or telephone number of an employee of an organization.

third party: An individual or organization outside of [INSERT NAME OF ORGANIZATION].

use: The treatment, handling, and management of personal information by and within [INSERT NAME OF ORGANIZATION] or by a third party with the knowledge and approval of [INSERT NAME OF ORGANIZATION].

The [INSERT NAME OF ORGANIZATION] Privacy Code in Detail

Principle 1 - Accountability

[INSERT NAME OF ORGANIZATION] is responsible for personal information under its control and shall designate one or more persons who are accountable for [INSERT NAME OF ORGANIZATION]'s compliance with the following principles.

- 1.1 Responsibility for compliance with the provisions of The [INSERT NAME OF ORGANIZATION] Privacy Code rests with the [INSERT NAME OF ORGANIZATION] Privacy Officer who can be reached at [INSERT 1-800 PHONE NUMBER] or via [INSERT E-MAIL]. Other individuals within [INSERT NAME OF ORGANIZATION] may be delegated to act on behalf of The [INSERT NAME OF ORGANIZATION] Privacy Officer or to take responsibility for the day-to-day collection and/or processing of personal information.
- 1.2 [INSERT NAME OF ORGANIZATION] shall make known, upon request, the title of the person or persons designated to oversee [INSERT NAME OF ORGANIZATION]'s compliance with The [INSERT NAME OF ORGANIZATION] Privacy Code.
- 1.3 [INSERT NAME OF ORGANIZATION] is responsible for personal information in its possession or control. [INSERT NAME OF ORGANIZATION] shall use contractual or other means to provide a comparable level of protection while information is being processed or used by a third party.
- 1.4 [INSERT NAME OF ORGANIZATION] shall implement policies and procedures to give effect to The [INSERT NAME OF ORGANIZATION] Privacy Code, including:
 - (a) implementing procedures to protect personal information and to oversee [INSERT NAME OF ORGANIZATION]'s compliance with The [INSERT NAME OF ORGANIZATION] Privacy Code;
 - (b) implementing procedures to receive and respond to complaints or inquiries;
 - (c) training and communicating to staff about [INSERT NAME OF ORGANIZATION]'s policies and procedures; and
 - (d) developing information materials to explain [INSERT NAME OF ORGANIZATION]'s policies and procedures.

Principle 2 - Identifying Purposes for Collection of Personal Information

[INSERT NAME OF ORGANIZATION] shall identify the purposes for which personal information is collected at or before the time the information is collected.

2.1 [INSERT NAME OF ORGANIZATION] collects personal information only for the following purposes:

[INSERT IDENTIFYING PURPOSES – LEGAL REVIEW NECESSARY]

Further reference to “identified purposes” mean the purposes identified in this Principle.

2.2 [INSERT NAME OF ORGANIZATION] shall specify orally, electronically or in writing the identified purposes to the [CLIENT/CUSTOMER] or employee at or before the time personal information is collected. Upon request, persons collecting personal information shall explain these identified purposes or refer the individual to a designated person within [INSERT NAME OF ORGANIZATION] who can explain the purposes.

2.3 When personal information that has been collected is to be used or disclosed for a purpose not previously identified, the new purpose shall be identified prior to use. Unless the new purpose is permitted or required by law, the consent of the [CLIENT/CUSTOMER] or employee will be acquired before the information will be used or disclosed for the new purpose.

Principle 3 - Obtaining Consent for Collection, Use or Disclosure of Personal Information

The knowledge and consent of a [CLIENT/CUSTOMER] or employee are required for the collection, use, or disclosure of personal information, except where inappropriate. In certain circumstances personal information can be collected, used, or disclosed without the knowledge and consent of the individual.

3.1 In obtaining consent, [INSERT NAME OF ORGANIZATION] shall use reasonable efforts to ensure that a [CLIENT/CUSTOMER] or employee is advised of the identified purposes for which personal information will be used or disclosed. The identified purposes shall be stated in a manner that can be reasonably understood by the [CLIENT/CUSTOMER] or employee.

3.2 Generally, [INSERT NAME OF ORGANIZATION] shall seek consent to use and disclose personal information at the same time it collects the information. However, [INSERT NAME OF ORGANIZATION] may seek consent to use and/or disclose personal information after it has been collected, but before it is used and/or disclosed for a new purpose.

3.3 [INSERT NAME OF ORGANIZATION] may require [CLIENTS/CUSTOMERS] to consent to the collection, use and/or disclosure of personal information as a condition of the supply of a product or service only if such collection, use and/or disclosure is required to fulfill the explicitly specified, and legitimate identified purposes.

3.4 In determining the appropriate form of consent, [INSERT NAME OF ORGANIZATION] shall take into account the sensitivity of the personal information and the reasonable expectations of its [CLIENTS/CUSTOMERS] and employees.

3.5 The purchase or use of products and services by a [CLIENT/CUSTOMER], or the acceptance of employment or benefits by an employee, may constitute implied consent for [INSERT NAME OF ORGANIZATION] to collect, use and disclose personal information for the identified purposes.

3.6 A [CLIENT/CUSTOMER] or employee may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. [CLIENTS/CUSTOMERS] and employees may contact [INSERT NAME OF ORGANIZATION] for more information regarding the implications of withdrawing consent.

- 3.7 [INSERT NAME OF ORGANIZATION] may collect or use personal information without knowledge or consent if it is clearly in the interests of the individual and consent cannot be obtained in a timely way, such as when the individual is seriously ill or mentally incapacitated.
- 3.8 [INSERT NAME OF ORGANIZATION] may collect, use or disclose personal information without knowledge or consent if seeking the consent of the individual might defeat the purpose of collecting, using or disclosing the information, such as in the investigation of a breach of an agreement or a contravention of a law.
- 3.9 [INSERT NAME OF ORGANIZATION] may collect, use or disclose personal information without knowledge or consent in the case of an emergency where the life, health or security of an individual is threatened.
- 3.10 [INSERT NAME OF ORGANIZATION] may use or disclose personal information without knowledge or consent to a lawyer representing [INSERT NAME OF ORGANIZATION], to collect a debt, to comply with a subpoena, warrant or other court order, or as may be otherwise required or authorized by law.

Principle 4 - Limiting Collection of Personal Information

[INSERT NAME OF ORGANIZATION] shall limit the collection of personal information to that which is necessary for the purposes identified by [INSERT NAME OF ORGANIZATION]. [INSERT NAME OF ORGANIZATION] shall collect personal information by fair and lawful means.

- 4.1 [INSERT NAME OF ORGANIZATION] collects personal information primarily from its [CLIENTS/CUSTOMERS] or employees.
- 4.2 [INSERT NAME OF ORGANIZATION] may also collect personal information from other sources including credit bureaus, employers or personal references, or other third parties who represent that they have the right to disclose the information.

Principle 5 - Limiting Use, Disclosure, and Retention of Personal Information

[INSERT NAME OF ORGANIZATION] shall not use or disclose personal information for purposes other than those for which it was collected, except with the consent of the individual or as required or permitted by law. [INSERT NAME OF ORGANIZATION] shall retain personal information only as long as necessary for the fulfillment of those purposes.

- 5.1 [INSERT NAME OF ORGANIZATION] may disclose a [CLIENT/CUSTOMER]'s personal information to:
- [INSERT POSSIBLE DISCLOSURES – LEGAL REVIEW NECESSARY]
- 5.2 [INSERT NAME OF ORGANIZATION] may disclose personal information about its employees to:
- [INSERT POSSIBLE DISCLOSURES – LEGAL REVIEW NECESSARY]
- 5.3 Only [INSERT NAME OF ORGANIZATION]'s employees with a business need-to-know, or whose duties reasonably so require, are granted access to personal information about [CLIENTS/CUSTOMERS] and employees.
- 5.4 [INSERT NAME OF ORGANIZATION] shall keep personal information only as long as it remains necessary or relevant for the identified purposes or as required by law. Depending on the circumstances, where personal information has been used to make a decision about a [CLIENT/CUSTOMER] or employee, [INSERT NAME OF ORGANIZATION] shall retain, for a period of time that is reasonably

sufficient to allow for access by the [CLIENT/CUSTOMER] or employee, either the actual information or the rationale for making the decision.

- 5.5 [INSERT NAME OF ORGANIZATION] shall maintain reasonable and systematic controls, schedules and practices for information and records retention and destruction which apply to personal information that is no longer necessary or relevant for the identified purposes or required by law to be retained. Such information shall be destroyed, erased or made anonymous.

Principle 6 - Accuracy of Personal Information

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

- 6.1 Personal information used by [INSERT NAME OF ORGANIZATION] shall be sufficiently accurate, complete, and up-to-date to minimize the possibility that inappropriate information may be used to make a decision about a [CLIENT/CUSTOMER] or employee.
- 6.2 [INSERT NAME OF ORGANIZATION] shall update personal information about [CLIENTS/CUSTOMERS] and employees as necessary to fulfill the identified purposes or upon notification by the individual.

Principle 7 - Security Safeguards

[INSERT NAME OF ORGANIZATION] shall protect personal information by security safeguards appropriate to the sensitivity of the information.

- 7.1 [INSERT NAME OF ORGANIZATION] shall protect personal information against such risks as loss or theft, unauthorized access, disclosure, copying, use, modification or destruction, through appropriate security measures, regardless of the format in which it is held.
- 7.2 [INSERT NAME OF ORGANIZATION] shall protect personal information disclosed to third parties by contractual agreements stipulating the confidentiality of the information and the purposes for which it is to be used.
- 7.3 All of [INSERT NAME OF ORGANIZATION]'s employees with access to personal information shall be required to respect the confidentiality of that information.

Principle 8 - Openness Concerning Policies and Procedures

[INSERT NAME OF ORGANIZATION] shall make readily available to [CLIENTS/CUSTOMERS] and employees specific information about its policies and procedures relating to the management of personal information.

- 8.1 [INSERT NAME OF ORGANIZATION] shall make information about its policies and procedures easy to understand, including:
- (a) the title and address of the person or persons accountable for [INSERT NAME OF ORGANIZATION]'s compliance with The [INSERT NAME OF ORGANIZATION] Privacy Code and to whom inquiries and/or complaints can be forwarded;
 - (b) the means of gaining access to personal information held by [INSERT NAME OF ORGANIZATION];
 - (c) a description of the type of personal information held by [INSERT NAME OF ORGANIZATION], including a general account of its use; and

- (d) a description of what personal information is made available to related organizations (e.g., subsidiaries).
- 8.2 [INSERT NAME OF ORGANIZATION] shall make available information to help [CLIENTS/CUSTOMERS] and employees exercise control of the collection, use and/or disclosure of their personal information and, where applicable, privacy-enhancing services available from [INSERT NAME OF ORGANIZATION].

Principle 9 - [CLIENT/CUSTOMER] and Employee Access to Personal Information

Upon request, [INSERT NAME OF ORGANIZATION] shall inform a [CLIENT/CUSTOMER] or employee of the existence, use, and disclosure of his or her personal information and shall give the individual access to that information. A [CLIENT/CUSTOMER] or employee shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

- 9.1 Upon request, [INSERT NAME OF ORGANIZATION] shall afford [CLIENTS/CUSTOMERS] and employees a reasonable opportunity to review the personal information in the individual's file. Personal information shall be provided in understandable form within a reasonable time, and at minimal or no cost to the individual.
- 9.2 In certain situations, [INSERT NAME OF ORGANIZATION] may not be able to provide access to all the personal information that it holds about a [CLIENT/CUSTOMER] or employee. For example, [INSERT NAME OF ORGANIZATION] may not provide access to information if doing so would likely reveal personal information about a third party or could reasonably be expected to threaten the life or security of another individual. Also, [INSERT NAME OF ORGANIZATION] may not provide access to information if disclosure would reveal confidential commercial information, if the information is protected by solicitor-client privilege, if the information was generated in the course of a formal dispute resolution process, or if the information was collected in relation to the investigation of a breach of an agreement or a contravention of the laws of Canada or a province.
- 9.3 Upon request, [INSERT NAME OF ORGANIZATION] shall provide an account of the use and disclosure of personal information and, where reasonably possible, shall state the source of the information. In providing an account of disclosure, [INSERT NAME OF ORGANIZATION] shall provide a list of third parties to which it may have disclosed personal information about the individual when it is not possible to provide an actual list.
- 9.4 In order to safeguard personal information, a [CLIENT/CUSTOMER] or employee may be required to provide sufficient identification information to permit [INSERT NAME OF ORGANIZATION] to account for the existence, use and disclosure of personal information and to authorize access to the individual's file. Any such information shall be used only for this purpose.
- 9.5 [INSERT NAME OF ORGANIZATION] shall promptly correct or complete any personal information found to be inaccurate or incomplete. Any unresolved differences as to accuracy or completeness shall be noted in the individual's file. Where appropriate, [INSERT NAME OF ORGANIZATION] shall transmit to third parties having access to the personal information in question any amended information or the existence of any unresolved differences.
- 9.6 [CLIENTS/CUSTOMERS] and employees can obtain information or seek access to their individual files by contacting the [INSERT NAME OF ORGANIZATION] Privacy Officer.

Principle 10 - Challenging Compliance

A [CLIENT/CUSTOMER] or employee shall be able to address a challenge concerning compliance with the above principles to the designated person or persons accountable for [INSERT NAME OF ORGANIZATION]'s compliance with The [INSERT NAME OF ORGANIZATION] Privacy Code.

- 10.1 [INSERT NAME OF ORGANIZATION] shall maintain procedures for addressing and responding to all inquiries or complaints from its [CLIENTS/CUSTOMERS] and employees regarding [INSERT NAME OF ORGANIZATION]'s handling of personal information.
- 10.2 [INSERT NAME OF ORGANIZATION] shall inform its [CLIENTS/CUSTOMERS] and employees about the existence of these procedures as well as the availability of complaint procedures.
- 10.3 The person or persons accountable for compliance with The [INSERT NAME OF ORGANIZATION] Privacy Code may seek external advice where appropriate before providing a final response to individual complaints.
- 10.4 [INSERT NAME OF ORGANIZATION] shall investigate all complaints concerning compliance with The [INSERT NAME OF ORGANIZATION] Privacy Code. If a complaint is found to be justified, [INSERT NAME OF ORGANIZATION] shall take appropriate measures to resolve the complaint including, if necessary, amending its policies and procedures. A [CLIENT/CUSTOMER] or employee shall be informed of the outcome of the investigation regarding his or her complaint.

Additional Information

For more information regarding The [INSERT NAME OF ORGANIZATION] Privacy Code, please contact the [INSERT NAME OF ORGANIZATION] Privacy Officer at [INSERT 1-800 PHONE NUMBER] or via [INSERT E-MAIL].

Please visit the Privacy Commissioner of Canada's web site at www.privcom.gc.ca.