

Strategic Analysis Corporation Code for the Protection of Personal Information

Principles in Summary

Ten interrelated principles form the basis of the Strategic Analysis Corporation ("SAC") code for the Protection of Personal Information. Each principle must be read in conjunction with the accompanying commentary.

1. **Accountability**

SAC is responsible for personal information under its control and has designated an individual (see 5.1 below) who is accountable for the organization's compliance with the policy principles.

2. **Identifying Purposes**

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

3. **Consent**

The knowledge and consent of the individuals 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 SAC. 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**

Security safeguards appropriate to the sensitivity of the information shall protect personal information.

8. **Openness**

SAC 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 accountable for SAC's compliance.

The ten principles that make up this Code are interrelated. SAC has adopted this Code and shall adhere to the ten principles as a whole.

Each of the principles is followed by a commentary on the principle. The commentaries are intended to help readers understand the significance and the implications of the principles. Where there is also a note following a principle (see principles 3 and 9), it forms an integral part of that principle.

Principles

Principle 1 – Accountability

SAC is responsible for personal information under its control and has designated an individual who is accountable for SAC's compliance with the following principles.

- i) Accountability for SAC's compliance with the principles rests with the designated individual, 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.
- ii) The identity of the individual designated by SAC to oversee its compliance with the principles is posted on SAC's website at the end of this document. It shall also be made known upon request.
- iii) SAC is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. SAC uses contractual or other means to provide a comparable level of protection while the information is being processed by a third party.
- iv) SAC has implemented policies and practices to give the 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 organizations policies; and
 - d) developing information to explain the organization's policies and procedures

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.

- i) SAC has documented the purposes for which personal information is collected in order to comply with the Openness principle and in the Individual Access principle.
- ii) Identifying the purposes for which personal information is collected at or before the time of collection will allow SAC on a continuing basis to determine the information it needs to collect to fulfill these purposes. The Limiting Collection principle (Principle 4) requires SAC to collect only that information necessary for the purposes that have been identified.
- iii) 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.

iv) 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 (Principle 3)

v) Persons collecting personal information will be able at all times to explain to individuals the purposes for which the information is being collected.

vi) This principle is linked closely to the Limiting Collection principle (Principle 4 and the Limiting Use, Disclosure, and Retention principle (Principle 5).

Principle 3 – Consent

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

Note: 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.

i) Consent is required for the collection of personal information and the subsequent use or disclosure of this information. Typically, SAC 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 SAC needs to use information for a purpose not previously identified).

ii) The principle requires “knowledge and consent”. SAC will 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.

iii) SAC may not, as a condition of the supply of a product or service, require an individual to consent to the collection, use or disclosure of information beyond that required to fulfill the explicitly specified, and legitimate purposes.

iv) The form of the consent sought by SAC may vary, depending upon the circumstances and the type of information. In determining the form of consent to use, SAC 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.

v) In obtaining consent, the reasonable expectations of the individual are also relevant. Consent shall not be obtained through deception. For example, an individual contacting SAC for information on their services should reasonably expect the SAC, in addition to using the individual's name and address for mailing purposes, would also contact the person to invite them to various company events. In this case, SAC will assume that the individual's original consent constitutes consent for such purpose.

vi) The way in which SAC seeks consent may vary, depending on the circumstances and the type of information collected. SAC will 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).

vii) 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) except where transfer of the information is required in order to supply appropriate services to the individual, a check off 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;
- d) consent may be given at the time that individuals use a service.

viii) An individual may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. Upon receiving a withdrawal notice, SAC will inform the individual of the implications of such withdrawal.

Principle 4 – Limiting Collection

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

i) SAC shall not collect personal information indiscriminately. Both the amount and the type of information collected shall be limited to that which is necessary to fulfill the purposes identified. SAC will specify the type of information collected as part of its information-handling policies and practices, in accordance with the Openness principle (Principle 8).

ii) This principle is linked closely to the Identifying Purposes principle (Principle 2) and the Consent principle (Principle 3)

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 fulfillment of those purposes.

i) SAC, when using personal information for a new purpose, shall document this purpose (see Principle 4 i).

ii) SAC has developed guidelines and implemented procedures with respect to the retention of personal information. These guidelines 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 information after the decision has been made. An organization may be subject to legislative requirements with respect to retention periods.

iii) Personal information that is no longer required to fulfill the identified purposes will be destroyed, erased, or made anonymous. SAC has developed guidelines and implemented procedures to govern the destruction of personal information.

iv) This principle is closely linked to the Consent principle (Principle 3), the Identifying Purposes principle (Principle 2), and the Individual Access principle (Principle 9).

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.

i) 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. The 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.

ii) SAC will complete routine updating of personal information only when such a process is necessary to fulfill the purposes for which the information was collected.

iii) 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.

Principle 7 – Safeguards

Personal information is protected by security safeguard appropriate to the sensitivity of the information.

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

ii) The nature of the safeguards 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. A higher level of protection safeguards more sensitive information. The concept of sensitivity is discussed in Principle 3 iv.

iii) The methods of protection include:

- a) physical measures, for example, locked filing cabinets and restricted access to offices;
- b) organization measures, for example, security clearances and limiting access on a “need-to-know” basis; and
- c) technological measures, for example, the use of passwords.

iv) SAC commits to make its employees aware of the importance of maintaining the confidentiality of personal information.

v) Care is used in the disposal or destruction of personal information, to prevent unauthorized parties from gaining access to the information (see Principle 5 iii).

Principle 8 – Openness

SAC shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

- i) SAC is open about its policies and practices with respect to the management of personal information. Individuals can acquire information about SAC's policies and practices simply by consulting its web site (www.strategicanalysis.ca) or by speaking to any member of its organization.
- ii) The information made available includes:
 - a) the name, title and address of the person who is accountable for SAC's policies and practices and to whom complaints or inquiries can be forwarded;
 - b) the means of gaining access to personal information held by SAC;
 - c) a description of the type of personal information held by SAC, including a general account of its use; and
 - d) what personal information is made available to related parties (eg. Head of Branch office; carrying broker).
- iii) SAC makes information on its policies and practices available in a variety of ways. For example, SAC makes paper copies available in its place of business on appointment; according to the inquirer's choice, information may be mailed; online access is also provided (www.strategicanalysis.ca); and finally, its toll-free telephone number may be used to request the information (1.877.214.5641).

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.

Note: In certain situations, SAC may not be able to provide access to all the personal information it holds about an individual. Exceptions to the access requirement are limited and specific. The reasons for denying access will be provided to the individual upon request. Exceptions may include information that contains references to other individuals, information that cannot be disclosed for legal, security, or commercial proprietary reasons, information that is prohibitively costly to provide and information that is subject to solicitor-client or litigation privilege.

- i) Upon request, SAC shall inform an individual whether or not it holds personal information about the individual. SAC will indicate the source of this information as long as that is documented. SAC shall allow the individual access to this information.

In addition, SAC will 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.

- ii) An individual may be required to provide sufficient information to permit SAC to provide an account of the existence, use, and disclosure of the personal information. The information provided shall only be used for this purpose.
- iii) In providing an account of third parties to which it has disclosed personal information about an individual, SAC will attempt to be as specific as possible. When it is not possible to provide a list of the third parties to which it has actually disclosed information about an

individual, SAC will provide a list of organizations to which it may have disclosed information about the individual.

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

v) When an individual successfully demonstrates the inaccuracy or incompleteness of personal information, SAC 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.

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

Principle 10 – Challenging Compliance

An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual accountable for SAC's compliance.

i) The individual accountable for an organization's compliance is discussed in Principle 1 i.

ii) SAC has put procedures in place to receive and respond to complaints or inquiries about its policies and practices relating to the handling of personal information. The complaint process is easily accessible and simple to use.

iii) SAC will inform individuals who make inquiries or lodge complaints of the existence of relevant complaint mechanisms.

iv) SAC will investigate all complaints. If a complaint is found to be justified through either the internal or external complaint review process, SAC shall take appropriate measures, including, if necessary, amending its policies and practices.

Nominative Information

SAC has appointed Ms. Wan Ying Kwun as the person accountable for its compliance with the above policy.