The 10 Principles of the CSA Model Code for the Protection of Personal Information

Please note: this brief is not exhaustive and does not constitute formal legal advice. The Canadian Chamber of Commerce urges you to consult legal counsel for further advice.

This brief focuses on the ten principles that make up the CSA Code

What is the Code and what is its status in the federal act?

The CSA Model Code for the Protection of Personal Information is a national standard that was developed by the Canadian Standards Association. It was developed in 1996, and resulted from a consensus between business representatives, consumer groups and government.

The Code is a central part of the federal act, PIPEDA. It forms Schedule 1 of the Act that outlines ten privacy principle organizations must follow when developing a privacy policy. To comply, you should make sure your organization builds an explicit privacy policy that addresses each of these principles.

In practice, the ten principles of the CSA Code may be read as steps to developing a privacy policy. In fact, organizations can use the code, with modifications to meet their specific needs, as their privacy policy. The ten principles, with explanatory notes, are as follows:

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.

Start by identifying internally who will be your privacy officer(s). As personal information may be collected and processed by different department within your business, you should also consider whether a team of individuals will be necessary to ensure your whole business in compliant with the Act.

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

Conduct a "privacy audit" to determine what personal information you collect and for what purpose. Consider specifically the nature of your customer relationship – there may be follow-on activity which may necessitate a broader purpose statement Check your forms and publications and/or websites to ensure privacy statements that identify purpose for collection of personal information are present and visible where necessary. Contact information for your privacy officer(s) should also be easily accessible.

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

Obtaining informed consent to collection is a central element of the Act. As part of your audit, consider how you collect information. As varying types of consent are possible, consider which is most appropriate to the nature, including sensitivity, of the information you collect.

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.

This means that an organization must limit the type of information collected to correspond to the stated purpose. Section 5(3) of PIPEDA includes a "reasonable person test" which mandates that organization can collect use or disclose personal information only for purposes that reasonable person would consider appropriate. This means you should consider which information is crucial for your purpose, and collect only that.

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.

This does not mean that you cannot outsource; however you cannot use or pass information on in a manner inconsistent with your identified purpose.
Your privacy policy must include guidelines that govern the handling of personal information while your organization is using it, including minimal and maximum times for retaining it. Information used to make a decision about an individual should also be kept sufficiently long enough to allow the individual to have access to it.

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.

Keep information as accurate as necessary, but note that the legislation prohibits routine updating if this is not necessary to fulfill the purpose given for the initial collection.

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

As part of your policy, put in place security policies and practices for storage of the information and for its disposal. Such practices can include physical or technical measures as needed, but also staff education and awareness.

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

Specific information, in an understandable form, on your information policies and practices must be readily available. This must include: name or title and address of the privacy officer; a description of the type of personal information an organization holds, including what it is generally used for; brochures or other information that explain the organizations' policies; what personal information is made available to related organization, such as subsidiaries.

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.

Keeping accurate records is necessary to ensure you are able to meet customer requests. Note that PIPEDA states that individual access requests must be made in writing, and that organization shall assist individuals that indicate they need help to prepare their requests. An organization must respond to a request, including to indicate that more time is need to process the request, within 30 days of receipt of the request.

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.

An organization must be ready to refer and act of complaints, including amending policies and practices if necessary. Be ready for compliance audits, which the Privacy Commissioner can undertake at his discretion, should be have reasonable grounds to believe the organization in contravention of the Act.