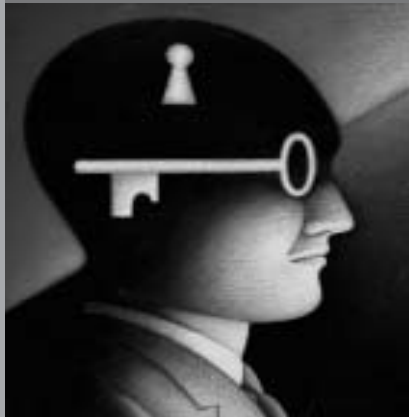


20 Questions

A SMALL BUSINESS SHOULD
ASK ABOUT *PRIVACY*



The Canadian Institute of Chartered Accountants
Innovations for a changing world



NATIONAL LIBRARY OF CANADA CATALOGUING IN PUBLICATION

20 questions a small business should ask about privacy

ISBN 1-55385-014-9

1. Privacy, Right of—Canada. 2. Personal information management—Canada. I. Canadian Institute of Chartered Accountants II. Title: Twenty questions a small business should ask about privacy.

KE4422.T84 2002 342.71'0858 C2002-905040-5
KF1262.T84 2002

Copyright © 2002

The Canadian Institute of Chartered Accountants

277 Wellington Street West

Toronto, Ontario

M5V 3H2

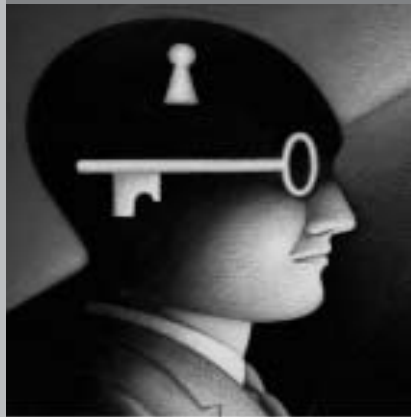
www.cica.ca/privacy

Printed in Canada

Disponible en français

20 Questions

A SMALL BUSINESS SHOULD
ASK ABOUT *PRIVACY*



The Canadian Institute of Chartered Accountants
Innovations for a changing world



20 Questions

A SMALL BUSINESS SHOULD ASK ABOUT *PRIVACY*

- 1 What personal information about customers and employees does your business collect and retain?
- 2 What personal information is used in carrying out business, for example, in sales, marketing, fundraising and customer relations?
- 3 What personal information does your business obtain from, or disclose to, affiliates or third parties, for example, in payroll outsourcing?
- 4 What is the impact of the PIPEDA, and/or provincial privacy requirements, on your business (a legal interpretation may be required)?
- 5 How does your business plan address the privacy of personal information?
- 6 To what degree is the owner/manager actively involved in the development, implementation and/or promotion of privacy measures?
- 7 Is the owner/manager able to assign an individual the responsibility for compliance with privacy legislation?
- 8 If so, has the individual responsible for privacy compliance been given clear authority to oversee the information handling practices of the business?
- 9 Are adequate resources allocated for developing, implementing and maintaining a privacy program?

- 10 What privacy policies has your business established with respect to the collection, use, disclosure and retention of personal information?
- 11 Where there are employees, how are the policies and procedures for managing personal information communicated to them?
- 12 How are the owner/manager and any employees with access to personal information trained in privacy protection?
- 13 Are the appropriate forms and documents fully developed?
- 14 To comply with established privacy policies, what specific objectives have been set for the business?
- 15 What are the consequences of not meeting the specific privacy objectives?
- 16 To what extent have appropriate privacy control measures been identified and implemented?
- 17 How is the effectiveness of the privacy control measures monitored and reported?
- 18 What mechanisms are in place to deal effectively with failures to properly apply the established privacy policies and procedures?
- 19 How would your business benefit from a comprehensive assessment of the risks, controls and business disclosures associated with personal information privacy?
- 20 Has the owner/manager considered the value-added services available from an independent assurance practitioner with respect to both offline and online privacy?



Introduction

Privacy is a significant concern to Canadian consumers. With identity theft, which Canada's Privacy Commissioner has called the fastest-growing crime in North America, and fears of financial or medical records being accessed inappropriately, consumers are worried that they have lost all control over their personal information. To address those concerns and to foster the growth of electronic commerce in Canada, the federal government enacted the *Personal Information Protection and Electronic Documents Act* (PIPEDA).

The PIPEDA came into force on January 1, 2001. It establishes new privacy rules to recognize the rights of individuals with respect to the collection, use, disclosure and retention of their personal information. The new rules also recognize the obligations of organizations to protect personal information in a manner that a reasonable person would consider appropriate in the circumstances.

Organizations are generally subject to the privacy rules if they collect, use or disclose personal information in the course of a commercial activity. In this regard, small businesses must establish a privacy program. By January 1, 2004, the privacy rights of all Canadians will be protected in one of two ways — by federal legislation or by provincial legislation that is “substantially similar” to the federal legislation.

The CICA's Information Technology Advisory Committee (ITAC) has developed this booklet to guide the owners/managers of small businesses in evaluating personal information privacy issues that might arise in discharging their responsibilities.

Owner/Manager Responsibilities for *Privacy*

Normally, the owner/manager of a small business is responsible for identifying the principal risks of the business and implementing appropriate measures to mitigate those risks. To determine the significance of privacy risk, it is important to conduct a privacy risk assessment. The results of that assessment will dictate whether, and to what extent, a privacy program should be established.

Personal information privacy risk can have a pervasive impact on a small business. For example, it can lead to:

- damage to the reputation of the business and the owner/manager, and to business relationships;
- legal liability and sanctions;
- charges of deceptive business practices;
- customer and employee distrust;
- denial of consent to use personal information for business purposes; and
- lost business and consequential reduction in sales and profits.

This booklet highlights key questions the owner/manager of a small business should ask with the aim of understanding privacy risk, implementing a privacy program, managing privacy risk and obtaining privacy assurance. The accompanying commentary is drawn from *Privacy Compliance: A Guide for Organizations & Assurance Practitioners*, also sponsored by ITAC. The Guide offers a framework that a small business can use to develop an appropriate privacy program. It also discusses the assurance practitioner's role in providing value-added services on privacy. Both the booklet and the guide are available free of charge on the CICA web site (www.cica.ca/privacy).

Questions About Information *Privacy*

Understanding Privacy Risk

Privacy has long been regarded as a basic human right in democratic societies. In Canada, a reasonable expectation of privacy might encompass:

- personal privacy (for example, physical and psychological privacy);
- privacy of space (for example, freedom from surveillance);
- privacy of communication (for example, freedom from monitoring and interception); and
- privacy of information (for example, control over the collection, use and disclosure of *personal information* by others).

The PIPEDA focuses on the privacy of personal information. It defines *personal information* as “information about an identifiable individual” that includes any factual or subjective information, recorded or not, in any form. Personal information might include, for example:

- name, identification numbers, income or blood type;
- evaluations, comments, social status or disciplinary actions;
- employee files, credit records, loan records, existence of a dispute between a consumer and a merchant, and intentions to acquire goods or services, or to change jobs.

Sensitive personal information is highlighted separately in the legislation. It might include, for instance, information on medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership and sexual preferences.

With respect to personal information, a small business should ask the following questions:

- 1 What personal information about customers and employees does your business collect and retain?
- 2 What personal information is used in carrying out business for example, in sales, marketing, fundraising and customer relations?
- 3 What personal information does your business obtain from, or disclose to, affiliates or third parties, for example, in payroll outsourcing?

The PIPEDA is groundbreaking legislation because it establishes Canada as the first country to implement private sector privacy rules based on national standards, the *Canadian Standards Association (CSA) Model Code for the Protection of Personal Information*. Formally launched in 1996, the CSA Model Code contains privacy principles that address the challenges businesses face in accommodating the personal information protection concerns of *customers and employees* and the varying circumstances under which personal information is collected and used for commercial purposes. The Model Code is technologically neutral, representing solid core principles that apply equally to paper-based files and electronic commerce.

To protect the privacy of personal information, prudent business practices call for a privacy risk assessment, either as part of an initial privacy review or when major changes are being proposed to existing business activities. Generally, activities that involve significant collection, use or disclosure of personally identifiable information should include such an assessment, and the results should be reflected in the business plan.

In the context of privacy risk assessment, a small business should ask two key questions:

- 4 **What is the impact of the PIPEDA, and/or provincial privacy requirements, on your business (a legal interpretation may be required)?**
- 5 **How does your business plan address the privacy of personal information?**

Implementing a Privacy Program

A sound privacy program requires clear leadership and a commitment by the owner/manager of a small business to prevent, detect and address noncompliance. Because the nature, size and complexity of operations will vary from one small business to another, a privacy program should be tailored to meet the needs of the individual business.

The PIPEDA requires that the responsibility for information privacy be assigned to someone, stating that: “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.” For small businesses, that person would often be the owner/manager because they understand how the business works, and its systems and

processes. The owner/manager, or another responsible individual, should determine whether the systems that store personal information have the capacity to track and record who has access to that information, for what purpose and under what conditions. In addition, the responsible individual should determine whether personal information has been disclosed to third parties and how such third parties are contractually or otherwise obligated to protect privacy.

A small business should ask the following questions about the privacy program:

- 6 To what degree is the owner/manager actively involved in the development, implementation and/or promotion of privacy measures?**
- 7 Is the owner/manager able to assign an individual the responsibility for compliance with privacy legislation?**
- 8 If so, has the individual responsible for privacy compliance been given clear authority to oversee the information handling practices of the business?**

The PIPEDA states that: “An organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances.” In this regard, the individual responsible for privacy compliance should take inventory of all personal information handling practices, including ongoing activities and new initiatives. A checklist may help to create the inventory by asking questions such as: What personal information is collected? Why is it collected? How is it collected? What is it used for? Where is it kept? Who has access? What security measures are used? To whom is it disclosed? When is it disposed of?

After completing the inventory of current privacy practices, the individual responsible for privacy compliance should determine what resources are needed for developing, implementing and maintaining a privacy program. When adequate resources are available, that individual should:

- prepare privacy policies and procedures, and communicate them to employees;
- train staff to manage and protect the privacy of personal information; and
- develop appropriate documents for disseminating information on privacy policies and prepare forms for responding to enquiries and complaints.

A small business should ask the following additional questions about the privacy program:

- 9 Are adequate resources allocated for developing, implementing and maintaining a privacy program?
- 10 What privacy policies has your business established with respect to the collection, use, disclosure and retention of personal information?
- 11 Where there are employees, how are the policies and procedures for managing personal information communicated to them?
- 12 How are the owner/manager and any employees with access to personal information trained in privacy protection?
- 13 Are the appropriate forms and documents fully developed?

Managing Privacy Risk

Privacy risk management is a continuous, evolving process that applies to all facets of the business. In applying the risk management process, a small business may establish a number of generic objectives in relation to the privacy principles set out in the CSA Model Code. Those principles encompass the following: accountability; identifying the purposes for the collection of personal information; obtaining consent; limiting collection; limiting use, disclosure and retention; ensuring accuracy; providing adequate security; making privacy policies readily available; providing individuals with access to their personal information; and enabling individuals to challenge an organization's compliance with its stated privacy policies.

Where a high level of risk exists, a specific objective or a set of sub-objectives may have to be established as well. In this regard, it is crucial for the owner/manager of a small business to identify the consequences of not meeting the established objectives and to specify the privacy control measures needed to prevent unacceptable risks, manage and monitor acceptable risks, and mitigate unexpected risks. Selecting appropriate control measures will depend on the nature and extent of the particular risks facing the small business. In addition, selection will require the exercise of judgment.

With respect to privacy risk management, several key questions should be asked:

- 14 **To comply with established privacy policies, what specific objectives have been set for the business?**
- 15 **What are the consequences of not meeting the specific privacy objectives?**
- 16 **To what extent have appropriate privacy control measures been identified and implemented?**
- 17 **How is the effectiveness of the privacy control measures monitored and reported?**
- 18 **What mechanisms are in place to deal effectively with failures to properly apply the established privacy policies and procedures?**

Obtaining Privacy Assurance

To enhance the trust relationships with customers, employees and third parties, and to fully comply with the spirit of the PIPEDA requirements, a small business faces a significant challenge — establishing and maintaining a comprehensive privacy risk management process.

In this regard, an independent assurance practitioner can support the owner/manager's commitment to privacy by providing value-added services, such as:

- developing a privacy philosophy and strategy;
- providing privacy advice and training;
- preparing and reviewing privacy policies;
- assessing and managing privacy risk;
- facilitating the development and implementation of privacy compliance programs, including privacy-enhancing technologies (such as the CICA WebTrust Seal of Assurance) to help protect online privacy; and
- providing assurance on the effectiveness of privacy control systems.

With regard to obtaining privacy assurance, a small business should ask the following questions:

- 19 **How would your business benefit from a comprehensive assessment of the risks, controls and business disclosures associated with personal information privacy?**
- 20 **Has the owner/manager considered the value-added services available from an independent assurance practitioner with respect to both offline and online privacy?**

CICA Information Technology Advisory Committee

CHAIR

Donald E. Sheehy, CA•CISA Grant Thornton LLP, Toronto

COMMITTEE

Gary S. Baker, CA, CISA Deloitte & Touche LLP, Toronto

David Chan, CA•CISA Toronto

Allan W.K. Cheung, CA, CISA The Canadian Depository for Securities Limited, Toronto

Henry Grunberg, CA Ernst & Young LLP, Toronto

Ray Henrickson, CA•CISA Bank of Nova Scotia, Toronto

Robert G. Parker, FCA, CA•CISA Deloitte & Touche LLP, Toronto

Douglas G. Timmins, CA Office of the Auditor General of Canada, Ottawa

Gerald D. Trites, FCA, CA•CISA St. Francis Xavier University, Antigonish, NS
(also staff consultant for the Committee)

Robert J. Widdowson, FCA KPMG LLP, Toronto

CICA STAFF

David J. Moore, CA

J. Paul-Émile Roy, CA

Gregory P. Shields, CA

Bryan C. Walker, CA

Cairine Wilson, MBA

ISBN 1-55385-014-9



9 781553 850144



20 Questions
A SMALL BUSINESS SHOULD
ASK ABOUT *PRIVACY*

277 Wellington Street West
Toronto, ON, Canada
M5V 3H2
Tel: 416-204-3306
Fax: 416-977-8585
www.cica.ca/privacy

Innovations for a changing world