General Instruction No. 1
CAN/CSA-Q830-96
March 1996

CSA Standard CAN/CSA-Q830-96, *Model Code for the Protection of Personal Information,* consists of **21 pages** (x preliminary and 11 text), each dated March 1996.

This Standard, like all CSA Standards, is subject to periodic review, and amendments in the form of replacement pages may be issued from time to time; such pages will be mailed automatically to those purchasers who complete and return the attached card.* Some Standards require frequent revision between editions, whereas others require none at all. It is planned to issue new editions of the Standard, regardless of the amount of revision, at intervals not greater than 5 years. Except in unusual circumstances, replacement pages will not be issued during the last year of that edition.

**This card will appear with General Instruction No. 1 only.*

Although any replacement pages that have been issued will be sold with the Standard, it is for the purchaser to insert them where they apply. The responsibility for ensuring that his or her copy is complete rests with the holder of the Standard, who should, for the sake of reference, retain those pages which have been replaced.

Note: *A General Instruction sheet will accompany replacement pages each time they are issued and will list the latest date of each page of the Standard.*

Cut along dotted line

Name _____

Organization _____

_____

Address _____

City _____

Province/State _____

Country _____ Postal/Zip Code _____

CAN/CSA-Q830-96

Place
Stamp
Here

Canadian Standards Association
Consolidated Mailing List
178 Rexdale Boulevard
Etobicoke, Ontario
Canada
M9W 1R3

National Standard of Canada *CAN/CSA-Q830-96*

Model Code for the Protection of Personal Information

Prepared by
Canadian Standards Association

Approved by
Standards Council of Canada

ISSN 0317-5669
Published in March 1996 by Canadian Standards Association
178 Rexdale Boulevard, Etobicoke, Ontario, Canada M9W 1R3

Technical Editor: *Dwayne Mathers*
Managing Editor: *Gary Burford*
Senior Project Editor: *Ann Martin*
Editor: *Maria Adragna*
Publishing System Operators: *Ursula Das/Grace DeStefano*

Contents

Technical Committee on Privacy

D. McKendry	Price Waterhouse, Ottawa, Ontario	*Chair*
J. Savary	York University, Toronto, Ontario	*Vice-Chair*
R. Binsell	Ministry of Consumer and Commercial Relations, Toronto, Ontario	
C. Black	Canadian Life & Health Insurance Association, Toronto, Ontario	
S. Blackwell	Canadian Radio-Television and Telecommunications, Commission, Hull, Québec	*Associate*
T. Campbell	Toronto, Ontario	*Associate*
A. Cavoukian	Information and Privacy Commissioner/Ontario, Toronto, Ontario	*Associate*
P. Chaves	Unitel Communications Inc., Toronto, Ontario	
J. Clayton	Public Works and Government Services Canada, Hull, Québec	*Associate*
A. Coles	AGT Limited, Edmonton, Alberta	
R. Crow	Information Technology Association of Canada, Mississauga, Ontario	
J.H. Deacon	Canada Post Corporation, Ottawa, Ontario	
D. Duncan	Information and Privacy Commissioner/Ontario, Toronto, Ontario	*Associate*
J. Ellis	Government Affairs, Credit Union Central of Canada, Ottawa, Ontario	*Associate*
B.J. Foran	Office of the Privacy Commissioner of Canada, Ottawa, Ontario	

A. Gibbons	Department of Finance, Ottawa, Ontario	
S. Gignac	Canadian Cable Television Association, Ottawa, Ontario	*Associate*
M. Globensky	Equifax Canada Inc., Ville d'Anjou, Québec	
J. Gustavson	Canadian Direct Marketing Association, Don Mills, Ontario	
W. Hanrahan	Information Technology Industry Council,, Washington, D.C., USA	*Associate*
C. Kniehl	Trust Companies Association of Canada, Toronto, Ontario	
G.H. Lavallée	Cable Television Standards Foundation, Ottawa, Ontario	
P. Lawson	Public Interest Advocacy Centre, Ottawa, Ontario	
P. Leduc	Industry Canada, Ottawa, Ontario	*Associate*
S.W. Lingard	Insurance Bureau of Canada, Toronto, Ontario	*Associate*
M. Long	Stentor Telecom Policy Inc., Ottawa, Ontario	
R. McGarry	Canadian Labour Congress, Ottawa, Ontario	
D. McInnes	Canadian Bankers Association, Ottawa, Ontario	
C. Mondello	Digital Equipment of Canada Limited, Nepean, Ontario	*Associate*
A.J. Neill	Department of Justice, Ottawa, Ontario	
P. Péladeau	Sociéte Progestacces, Montréal, Québec	

S. Perrin	Industry Canada, Ottawa, Ontario	
D. Pye	Westmount Research Consultants Inc., Toronto, Ontario	
R. Poirier	Canadian Wireless Telecommunications Association, Ottawa, Ontario	*Associate*
P. Racine	Heritage Canada, Ottawa, Ontario	*Associate*
B. Robins	The Reader's Digest Association (Canada) Ltd., Westmount, Québec	
E. Rothberg	Life Underwriters Association of Canada, Don Mills, Ontario	*Associate*
L. Routledge	Canadian Bankers Association, Toronto, Ontario	*Associate*
M.A. Stevens	Treasury Board Secretariat, Ottawa, Ontario	*Associate*
F. Swedlove	Department of Finance, Ottawa, Ontario	*Associate*
J. Tobin	American Express Company, New York, New York, USA	
M. Vallée	Fédération nationale des associations, de consommateurs du Québec, Montréal, Québec	
K. Webb	Industry Canada, Ottawa, Ontario	
D.D. Mathers	Canadian Standards Association, Etobicoke, Ontario	*Administrator*

For further information, contact

R. Haighton	Canadian Standards Association, Etobicoke, Ontario	

Preface

This is the first edition of CSA Standard CAN/CSA-Q830, *Model Code for the Protection of Personal Information.*

This Standard was prepared by the CSA Technical Committee on Privacy, under the jurisdiction of the CSA Steering Committee on Business Management Systems, and was formally approved by these Committees. It has been approved as a National Standard of Canada by the Standards Council of Canada.

March 1996

Notes:
(1) *Use of the singular in this Standard does not exclude the plural (and vice versa) when the sense allows.*
(2) *Although the intended primary application of this Standard is stated in its Scope, it is important to note that it remains the responsibility of the users of the Standard to judge its suitability for their particular purpose.*
(3) *This publication was developed by consensus, which is defined by* CSA Regulations Governing Standardization *as "substantial agreement reached by concerned interests. Consensus includes an attempt to remove all objections and implies much more than the concept of a simple majority, but not necessarily unanimity." It is consistent with this definition that a member may be included in the Technical Committee list and yet not be in full agreement with all clauses of the publication.*
(4) *CSA Standards are subject to periodic review, and suggestions for their improvement will be referred to the appropriate committee.*
(5) *All enquiries regarding this Standard, including requests for interpretation, should be addressed to Canadian Standards Association, Standards Development, 178 Rexdale Boulevard, Etobicoke, Ontario M9W 1R3.*
Requests for interpretation should
(a) define the problem, making reference to the specific clause, and, where appropriate, include an illustrative sketch;
(b) provide an explanation of circumstances surrounding the actual field condition; and
(c) be phrased where possible to permit a specific "yes" or "no" answer.
Interpretations are published in CSA's periodical Info Update. *For subscription details, write to CSA Sales Promotion,* Info Update, *at the address given above.*

Introduction

Canada is part of a global economy based on the creation, processing, and exchange of information. The technology underlying the information economy provides a number of benefits that improve the quality of our lives. This technology also gives rise to concerns about the protection of privacy rights and the individual's right to control the use and exchange of personal information. By implementing recognized fair-handling practices for personal information, organizations can materially demonstrate their commitment to the protection of personal information. Organizations should balance their need for personal information with an individual's desire for a certain measure of anonymity.

This document is a voluntary national standard for the protection of personal information. The Standard addresses two broad issues: the way organizations collect, use, disclose, and protect personal information; and the right of individuals to have access to personal information about themselves, and, if necessary, to have the information corrected. Ten interrelated principles form the basis of the Standard. Each principle is accompanied by a commentary that elaborates on the principle.

A workbook on the implementation of the principles is available to organizations intending to adopt this Standard. Organizations will be able to tailor specific codes using the workbook as a guide.

This Standard will

(a) provide principles for the management of personal information;

(b) specify the minimum requirements for the adequate protection of personal information held by participating organizations;

(c) make the Canadian public aware of how personal information should be protected; and

(d) provide standards by which the international community can measure the protection of personal information in Canada.

Canada committed itself to privacy protection in 1984 by signing the Organization for Economic Co-operation and Development (OECD) *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.* The OECD *Guidelines* (see Appendix A) were used as the basis for the development of this Standard. The protection of personal information is increasingly important at the international level.

Principles in Summary

Ten interrelated principles form the basis of the CSA Model Code for the Protection of Personal Information. Each principle must be read in conjunction with the accompanying commentary.

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 fulfilment 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
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.

CAN/CSA-Q830-96
Model Code for the Protection of Personal Information

1. Scope

1.1
This model code describes the minimum requirements for the protection of personal information. Any applicable legislation must be considered in implementing these requirements.

1.2
This Standard may be applied to all personal information. Provided the minimum requirements are met, organizations may tailor this Standard to meet their specific circumstances. For example, policies and practices may vary, depending upon whether the personal information relates to members, employees, customers, or other individuals.

1.3
The objective of this Standard is to assist organizations in developing and implementing policies and practices to be used when managing personal information.

2. Definitions

2.1
The following definitions apply in this Standard:

Collection — the act of gathering, acquiring, or obtaining personal information from any source, including third parties, by any means.

Consent — voluntary agreement with what is being done or proposed. Consent can be either express or implied. Express consent is given explicitly, either orally or in writing. Express consent is unequivocal and does not require any inference on the part of the organization seeking consent. Implied consent arises where consent may reasonably be inferred from the action or inaction of the individual.

Disclosure — making personal information available to others outside the organization.

Organization — a term used in the model code that includes associations, businesses, charitable organizations, clubs, government bodies, institutions, professional practices, and unions.

Personal information — information about an identifiable individual that is recorded in any form.

Use — refers to the treatment and handling of personal information within an organization.

3. General Requirements

3.1

The ten principles that make up this Standard are interrelated. Organizations adopting this Standard shall adhere to the ten principles as a whole.

3.1.1

Organizations may tailor this Standard to meet their particular circumstances by
(a) defining how they subscribe to the ten principles;
(b) developing an organization-specific code; and
(c) modifying the commentary to provide organization-specific examples.

3.1.2

Each of the principles is followed by a commentary on the principle. The commentaries are intended to help individuals and organizations 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 the principle.

3.1.3

Although the following clauses use prescriptive language (ie, the words "shall" or "must"), this document is a **voluntary** standard. Should an organization choose to adopt the principles and general practices contained in this Standard, the clauses containing prescriptive language become requirements. The use of the word "should" indicates a recommendation.

4. Principles

4.1 Principle 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.

4.1.1

Accountability for the organization's compliance with the principles rests with the designated individual(s), 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(s).

4.1.2

The identity of the individual(s) designated by the organization to oversee the organization's compliance with the principles shall be made known upon request.

4.1.3

An organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organization should use contractual or other means to provide a comparable level of protection while the information is being processed by a third party.

4.1.4
Organizations shall implement policies and practices to give 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 organization's policies and practices; and
(d) developing information to explain the organization's policies and procedures.

4.2 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.

4.2.1
The organization shall document the purposes for which personal information is collected in order to comply with the Openness principle (Clause 4.8) and the Individual Access principle (Clause 4.9).

4.2.2
Identifying the purposes for which personal information is collected at or before the time of collection allows organizations to determine the information they need to collect to fulfil these purposes. The Limiting Collection principle (Clause 4.4) requires an organization to collect only that information necessary for the purposes that have been identified.

4.2.3
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.

4.2.4
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 (Clause 4.3).

4.2.5
Persons collecting personal information should be able to explain to individuals the purposes for which the information is being collected.

4.2.6
This principle is linked closely to the Limiting Collection principle (Clause 4.4) and the Limiting Use, Disclosure, and Retention principle (Clause 4.5).

4.3 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. In addition, organizations that do not have a direct relationship with the individual may not always be able to seek consent. For example, seeking consent may be impractical for a charity or a direct-marketing firm that wishes to acquire a mailing list from another organization. In such cases, the organization providing the list would be expected to obtain consent before disclosing personal information.

4.3.1

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

4.3.2

The principle requires "knowledge and consent". Organizations shall 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.

4.3.3

An organization 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 fulfil the explicitly specified, and legitimate purposes.

4.3.4

The form of the consent sought by the organization may vary, depending upon the circumstances and the type of information. In determining the form of consent to use, organizations 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. For example, the names and addresses of subscribers to a newsmagazine would generally not be considered sensitive information. However, the names and addresses of subscribers to some special-interest magazines might be considered sensitive.

4.3.5

In obtaining consent, the reasonable expectations of the individual are also relevant. For example, an individual buying a subscription to a magazine should reasonably expect that the organization, in addition to using the individual's name and address for mailing and billing purposes, would also contact the person to solicit the renewal of the subscription. In this case, the organization can assume that the individual's request constitutes consent for specific purposes. On the other hand, an individual would not reasonably expect that personal information given to a health-care professional would be given to a company selling health-care products, unless consent were obtained. Consent shall not be obtained through deception.

4.3.6

The way in which an organization seeks consent may vary, depending on the circumstances and the type of information collected. An organization should 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).

4.3.7
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) a checkoff 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; or
(d) consent may be given at the time that individuals use a product or service.

4.3.8
An individual may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. The organization should inform the individual of the implications of such withdrawal.

4.4 Principle 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.

4.4.1
Organizations shall not collect personal information indiscriminately. Both the amount and the type of information collected shall be limited to that which is necessary to fulfil the purposes identified. Organizations should specify the type of information collected as part of their information-handling policies and practices, in accordance with the Openness principle (Clause 4.8).

4.4.2
The requirement that personal information be collected by fair and lawful means is intended to prevent organizations from collecting information by misleading or deceiving individuals about the purpose for which information is being collected. This requirement implies that consent with respect to collection must not be obtained through deception.

4.4.3
This principle is linked closely to the Identifying Purposes principle (Clause 4.2) and the Consent principle (Clause 4.3).

4.5 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 fulfilment of those purposes.

4.5.1
Organizations using personal information for a new purpose shall document this purpose (see Clause 4.2.1).

4.5.2
Organizations should develop guidelines and implement procedures with respect to the retention of personal information. These guidelines should 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 the information after the decision has been made. An organization may be subject to legislative requirements with respect to retention periods.

4.5.3
Personal information that is no longer required to fulfil the identified purposes should be destroyed, erased, or made anonymous. Organizations should develop guidelines and implement procedures to govern the destruction of personal information.

4.5.4
This principle is closely linked to the Consent principle (Clause 4.3), the Identifying Purposes principle (Clause 4.2), and the Individual Access principle (Clause 4.9).

4.6 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.

4.6.1
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. 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.

4.6.2
An organization should not routinely update personal information, unless such a process is necessary to fulfil the purposes for which the information was collected.

4.6.3
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.

4.7 Principle 7 — Safeguards
Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

4.7.1
The security safeguards shall protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification. Organizations shall protect personal information regardless of the format in which it is held.

4.7.2
The nature of the safeguards will 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. More sensitive information should be safeguarded by a higher level of protection. The concept of sensitivity is discussed in Clause 4.3.4.

4.7.3
The methods of protection should include
(a) physical measures, for example, locked filing cabinets and restricted access to offices;
(b) organizational measures, for example, security clearances and limiting access on a "need-to-know" basis; and
(c) technological measures, for example, the use of passwords and encryption.

4.7.4
Organizations shall make their employees aware of the importance of maintaining the confidentiality of personal information.

4.7.5
Care shall be used in the disposal or destruction of personal information, to prevent unauthorized parties from gaining access to the information (see Clause 4.5.3).

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

4.8.1
Organizations shall be open about their policies and practices with respect to the management of personal information. Individuals should be able to acquire information about an organization's policies and practices without unreasonable effort. This information shall be made available in a form that is generally understandable.

4.8.2
The information made available shall include
(a) the name/title and address of the person who is accountable for the organization's policies and practices and to whom complaints or inquiries can be forwarded;
(b) the means of gaining access to personal information held by the organization;
(c) a description of the type of personal information held by the organization, including a general account of its use;
(d) a copy of any brochures or other information that explain the organization's policies, standards, or codes; and
(e) what personal information is made available to related organizations (eg, subsidiaries).

4.8.3
An organization may make information on its policies and practices available in a variety of ways. The method chosen depends on the nature of its business and other considerations. For example, an organization may choose to make brochures available in its place of business, mail information to its customers, provide online access, or establish a toll-free telephone number.

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

4.9.1

Upon request, an organization shall inform an individual whether or not the organization holds personal information about the individual. Organizations are encouraged to indicate the source of this information. The organization shall allow the individual access to this information. However, the organization may choose to make sensitive medical information available through a medical practitioner. In addition, the organization should 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.

4.9.2

An individual may be required to provide sufficient information to permit an organization to provide an account of the existence, use, and disclosure of personal information. The information provided shall only be used for this purpose.

4.9.3

In providing an account of third parties to which it has disclosed personal information about an individual, an organization should attempt to be as specific as possible. When it is not possible to provide a list of the organizations to which it has actually disclosed information about an individual, the organization should provide a list of organizations to which it may have disclosed information about the individual.

4.9.4

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

4.9.5

When an individual successfully demonstrates the inaccuracy or incompleteness of personal information, the organization 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.

4.9.6

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.

4.10 Principle 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.

4.10.1

The individual accountable for an organization's compliance is discussed in Clause 4.1.1.

4.10.2

Organizations shall put procedures in place to receive and respond to complaints or inquiries about their policies and practices relating to the handling of personal information. The complaint process should be easily accessible and simple to use.

4.10.3

Organizations shall inform individuals who make inquiries or lodge complaints of the existence of relevant complaint mechanisms. A range of these mechanisms may exist. For example, some regulatory bodies accept complaints about the personal-information handling practices of the companies they regulate.

4.10.4

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

Appendix A
Organization for Economic Co-operation and Development, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data

Notes:
(1) *This Appendix is not a mandatory part of this Standard.*
(2) *Canada adhered to these Guidelines in 1984. They were used as the basis for the development of the CSA Model Code for the Protection of Personal Information.*

Collection Limitation Principle
There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

Data Quality Principle
Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

Purpose Specification Principle
The purpose for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

Use Limitation Principle
Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 (Purpose Specification Principle) except:
(a) with the consent of the data subject; or
(b) by the authority of law.

Security Safeguards Principle
Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.

Openness Principle
There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

Individual Participation Principle
An individual should have the right:
(a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;
(b) to have communicated to him, data relating to him
  (i) within a reasonable time;
  (ii) at a charge, if any, that is not excessive;
  (iii) in a reasonable manner; and
  (iv) in a form that is readily intelligible to him;

(c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and
(d) to challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed or amended.

Accountability Principle
A data controller should be accountable for complying with measures which give effect to the principles stated above.

Proposal for Change

To help our volunteer members to assess proposals to change requirements we recommend that each proposal for change be submitted in writing and identify the
(a) Standard number;
(b) Clause number;
(c) proposed wording of the Clause (requirement, test, or pass/fail criterion) using mandatory language and underlining those words changed from the existing Clause (if applicable); and
(d) rationale for the change, including all supporting data necessary to be considered.

The proposal should be submitted to the Standards Administrator at least one month prior to the next meeting of the Committee. It is CSA Committee practice that only those proposals sent out to members prior to a meeting can be the subject of discussion and action. This is to allow the members time to consider the proposal and to do any research they may feel necessary.

Date: ____ - ____ - ____
YY MM DD

To: The Standards Administrator of CSA Standard _____

From: _____

Affiliation: _____

Address: _____

_____

Phone: _____ **Fax:** _____

Re: Request for an Amendment, Deletion, or Addition to Clause(s) _____

Proposed change:

(Use reverse and additional pages as required.)

Product Description Produit	Quantity Nombre	Price Prix	Sub-Total Total	Shipping (see chart) Frais de port (voir grille)	Sub-Total Total	GST* TPS*	PST** TVP**	Sub-Total Total	QST*** TVQ***	Sub-Total Total
	x	=	+	=	+	+	=	+	=	
	x	=	+	=	+	+	=	+	=	
	x	=	+	=	+	+	=	+	=	
	x	=	+	=	+	+	=	+	=	
	x	=	+	=	+	+	=	+	=	

Grand Total/Total global :

* Add GST to all Canadian Orders. (NOTE: The CE Code Handbook and all PLUS products are GST exempt.) / Ajouter la TPS à toute commande passée au Canada. (NOTE. Le Guide explicatif du CCE et les répertoires sont exempts de TPS.)
** Add PST on all orders for electronic products placed in Alberta, British Columbia, Manitoba, New Brunswick or Ontario. / Ajouter la TVP à toute commande de produits électroniques passée en Alberta, en Colombie-Britannique, au Manitoba, au Nouveau Brunswick et en Ontario.
*** Add QST to all Quebec orders. (NOTE: The CE Code Handbook and all PLUS products are QST exempt.) / Ajouter la TVQ à toute commande passée au Québec. (NOTE. Le Guide explicatif du CCE et les répertoires sont exempts de TVQ.)

SHIP TO • EXPÉDIER À

If billing address is different, please specify.
Si la facture doit être envoyée à une autre adresse, veuillez l'indiquer.

Name / Nom

Title / Titre

Organization / Entreprise

Address / Adresse

City / Ville

Prov. / State / Prov. / État

Country / Pays

Postal / Zip code / Code postal

Telephone / Téléphone

SM or CM NO. / N° MS ou MC[1]

[1] Note. Discount applicable only if sustaining or certification No. provided.
La remise est accordée uniquement si le n° de membre de soutien ou de certification est donné.

Shipping and Handling • Frais de port et d'emballage

Product	Canada	United States États-Unis	Other Countries
...ns ...imées	$4/copy 4 $/exemplaire	$6/... 6 $/...	
	$60/year 60 $/année	$60/year 60 $/année	
	/copy /exemplaire	$15/copy 15 $/exemplaire	

...first class mail unless other...

...ication... ...imées ... ...e par ... ...r de l'... ...se, et les
...e messa... ...e.
..., par transport aérien ou terrestre, peut faire l'objet de ... ...e
...nt payables par le destinataire et sont basés sur la valeur déclarée de l'envoi.

METHOD OF PAYMENT • MODALITÉS DE PAIEMENT

All first-time orders are to be paid by cash, cheque or credit card.
Toute commande initiale doit être payée comptant, par chèque ou par carte de crédit.

1 Purchase Order No. • Bon d'achat n°
(North America only/Amérique du Nord seulement)

2 CSA Customer No. • N° de client CSA

3 Payment enclosed $ • Montant inclus $
Make cheque payable to Canadian Standards Association. / Le chèque doit être fait à l'ordre de l'Association canadienne de normalisation.

4 Charge to credit card indicated • Porter à mon compte :

☐ American Express ☐ Visa ☐ Master Card Expiration date/Date d'expiration

Carte n°

Card holder's name • Nom du titulaire

Signature

Order Form Bon de commande

Std

Association Activities

The Canadian Standards Association is a not-for-profit, independent, private sector organization that serves the public, governments, and business as a forum for national consensus in the development of standards, and offers them certification, testing, and related services. It is a membership Association open to any individual, company, or organization interested in standards activities.

The more than 1000 standards published by CSA are written, reviewed, and revised by over 7000 committee members, who represent users, producers, and regulatory authorities in all regions of Canada. In addition to these volunteers, some 2000 representatives from industry, labour, governments, and the public participate in the work of the Association through sustaining memberships. Approximately one-third of CSA's standards have been referenced into law by provincial and federal authorities.

Activities in the standards field cover a number of program areas: lifestyles and the environment, electrical/electronics, construction, energy, transportation/distribution, materials technology, business/production management systems, communications/information technology, and welding. These are all listed in our catalogue, which is available on request.

We welcome your comments and inquiries. Further information on standards programs may be obtained by writing to

The Director, Standards Programs
Standards Development
Canadian Standards Association
178 Rexdale Boulevard
Etobicoke, Ontario
Canada
M9W 1R3