



Aviva Canada Inc. Privacy Policy

Taking care of what's **important** to *you*

Table of Contents

- [Introduction](#)
- [Privacy in Canada](#)
- [Definition of Personal Information](#)
- [Privacy Policy: the ten principles](#)
- [Accountability](#)
- [Identifying Purposes](#)
- [Consent](#)
- [Limiting Collection](#)
- [Limiting Use, Disclosure, and Retention](#)
- [Accuracy](#)
- [Safeguards](#)
- [Openness](#)
- [Customer Access](#)
- [Challenging Compliance](#)

- [Appendix](#)
- [Federal Privacy Commissioner](#)
- [How to contact Aviva's Privacy Officer](#)

Updated September 1, 2007

Introduction

At Aviva, we are committed to protecting and keeping private our policyholders' and partners' personal information. Our Privacy Policy sets out principles on the collection, protection, use and disclosure of personal information. All employees are required to comply with the Privacy Policy in the execution of their daily activities.

Personal information is collected by Aviva and its representatives for the purposes of establishing and maintaining communications with customers; assessing insurance applications including underwriting and pricing policies; verifying information; investigating and paying claims; detecting and preventing fraud; analyzing business results; and acting as required or authorized by the law.

Aviva identifies to our customers the rationale for collecting the personal information at or prior to its actual collection. Our consumers in turn must consent to its collection implicitly, or expressly. It's our promise to ensure that the personal information collected on our customers is only used for the purpose for which it was originally intended.

We take our commitment to protecting personal information seriously. For more information, please review the content of this website.

Robin Spencer
President and Chief Executive Officer

Privacy in Canada

Federal Legislation: Personal Information Protection and Electronic Documents Act

The *Personal Information Protection and Electronic Documents Act* (PIPEDA) sets standards and regulations governing the collection, use and disclosure of personal information by private sector organizations.

This law impacts the way private corporations, federal agencies, not-for-profit organizations and associations handle personal information. At the same time, it clearly establishes a code of practices to ensure that the personal information of Canadians is handled respectfully and privately.

PIPEDA is based on ten principles established by the Canadian Standards Association's *Model Code for the Protection of Personal Information* (CSA Model Code). These principles were recognized as a Canadian standard in 1996 and address the ways in which organizations should collect, use, and disclose personal information. They also address an individual's right to access his/her personal information and his/her right to have it amended where appropriate.

The federal law was implemented in three stages. The first stage, which came into effect on January 1, 2001, affected federally-regulated organizations including Canadian banks and airlines, and organizations that collect, use, or disclose personal information for profit on an inter-provincial or international basis. On January 1, 2002, this law was extended to cover personal health information. On January 1, 2004, most organizations regardless of their size, which collect, use or disclose personal information in the course of commercial activity, became subject to the provisions of this Act.

Privacy in Canada

Provincial Legislation

The province of Quebec was the first jurisdiction in North America to enact comprehensive personal information protection legislation for the private sector. *An Act respecting the Protection of Personal Information in the Private Sector* sets out fair information practices for businesses operating in Quebec.

The provinces of Alberta and British Columbia enacted their own privacy laws, the *Personal Information Protection Act* of British Columbia and the *Personal Information Protection Act* of Alberta, on January 1, 2004.

As other provinces enact similar legislation, organizations conducting commercial activity within a province will be subject to the provisions of their provincial laws rather than PIPEDA. However, PIPEDA will continue to regulate cross-border, inter-provincial and international trade and commerce.

Definition of Personal Information

“Personal Information” is defined as information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization. This is a very broad definition and may encompass most types of information held such as race, medical, criminal, employment and financial history. The legislation only applies to information collected, used or disclosed in the course of commercial dealings.

It also includes, for example, an individual's address, telephone number, date of birth, family status, marital status, occupation, medical and health records, assets, liabilities, income, credit rating, credit and payment records, an individual's previous insurance experience including claims history, individual's driving record, policy number and vehicle identity number.

However, Personal Information does not include certain prescribed sources of public information such as:

- Personal Information consisting of the name, address and telephone number of a subscriber that appears in a telephone directory that is available to the public, where the subscriber can refuse to have the Personal Information appear in the directory;
- Personal Information including the name, title, address and telephone number of the individual that appears in a professional or business directory, listing or notice, that is available to the public, where the collection use and disclosure of the Personal Information relates directly to the purpose for which the information appears in the directory, listing or notice;
- Personal Information that appears in a registry collected under statutory authority and to which a right of public access is authorized by law, where the collection, use and disclosure the Personal Information relate directly to the purpose for which the information appears in the registry;
- Personal Information that appears in a record or document of a judicial or quasi-judicial body, that is available to the public, where the collection and disclosure of the Personal Information relates directly to the purpose for which the information appears in the record or document; and
- Personal Information that appears in a publication, including a magazine, book or newspaper, in printed or electronic form, that is available to the public, where the individual has provided the information.

Aviva's Privacy Policy: the ten principles

The objective of our Privacy Policy is to ensure the protection of Aviva customers' Personal Information. This includes Personal Information residing within Aviva and

Personal Information provided to other third parties in the conduct of commercial activities. To attain this goal, Aviva complies with the following principles:

- Aviva is responsible for Personal Information under its possession, custody, or control and a designated Privacy Officer is accountable for Aviva's compliance to Privacy Policy and Procedures. [\[Principle One\]](#)
- Aviva shall inform individuals of the purposes for which Personal Information is collected at or before the time the information is collected. [\[Principle Two\]](#)
- Aviva requires the knowledge and consent of the individual for the collection, use, or disclosure of Personal Information, except in certain circumstances where consent is not required. [\[Principle Three\]](#)
- Aviva shall only collect Personal Information that is necessary for the identified purposes and such information shall be collected by fair and lawful means. [\[Principle Four\]](#)
- Aviva 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. Aviva shall only retain Personal Information as long as necessary for the fulfillment of such purposes. [\[Principle Five\]](#)
- Aviva shall ensure that Personal Information is as accurate, complete, and up-to-date as deemed necessary for the purposes for which it is to be used. [\[Principle Six\]](#)
- Aviva shall protect Personal Information by establishing and operating security safeguards appropriate to the sensitivity of the information, which is held, and to prevent any unauthorized activity relative to the information. [\[Principle Seven\]](#)
- Upon request, Aviva shall make readily available to individuals specific information about its policy and procedures and complaints handling process relating to the management of Personal Information and complaints handling process. [\[Principle Eight\]](#)
- Upon request, Aviva shall inform an individual of the existence, use, and disclosure of any Personal Information retained by Aviva about them and they shall be given access to the information, except as may be limited by law. Aviva shall amend Personal Information as deemed appropriate to ensure continued accuracy. [\[Principle Nine\]](#)
- Aviva shall provide a means for individuals to challenge compliance with the above with Aviva's Privacy Officer. [\[Principle Ten\]](#).

ONE: Accountability

Aviva is responsible for Personal Information under its possession, custody or control and a designated Privacy Officer is accountable for Aviva's compliance to the Privacy Policy and Procedures.

We are responsible for all Personal Information under our control, whether supplied to us directly by you or by a third party, or that we have provided to a third party for processing.

We have established policies and procedures to comply with our Privacy Policy, and have designated a Privacy Officer who is responsible for ensuring we comply with privacy legislation.

Please click [here](#) to contact our Privacy Officer regarding your specific privacy questions or concerns.

TWO: Identifying Purposes

Aviva shall inform individuals of the purposes for which Personal Information is collected at or before the time the information is collected.

When you apply for a service or product, Aviva shall only use your Personal Information to:

- Communicate with you
- Assess your insurance applications including underwriting and pricing policies
- Verify your information with government agencies, brokers, agents, insurers, other insurance reporting agencies and credit bureaus
- Investigate and settle claims
- Detect and prevent fraud
- Analyze business results, compile statistics and conduct marketing and underwriting research and modeling
- Act as required or authorized by law

Aviva may also offer and/or provide products and services to meet your needs unless otherwise notified. If we require your Personal Information for any other purpose, Aviva will seek your consent prior to using it.

THREE: Consent

Aviva requires the knowledge and consent of the individual for the collection, use, or disclosure of their Personal Information, except in certain circumstances where consent is not required.

General

We issue an insurance policy with the understanding that, in addition to providing your consent, you have obtained the consent from all persons named in your insurance policy

for the collection, use and disclosure of their Personal Information, for the purposes outlined above.

Obtaining Consent

You can provide consent to the collection, use and disclosure of your Personal Information expressly or implicitly.

Express consent can be given orally or in writing. It is given by agreement or action on the part of the customer, to acquire or accept a product or service. For example, express oral consent can be given over the telephone, or express written consent can be given by signing an application form or an agreement which may relate to Personal Information. Express consent by an action can be given by clicking an accept button on a computer screen. If oral express consent is given, Aviva will document and/or record the conversation, specifically the name, date, and details of the conversation in either hard or soft copy within the appropriate policy or claim file documentation in order that it may be easily located and accessed should this be necessary.

Consent will also be given by you and accepted by us when you are provided our privacy notice along with your policy and you do not advise that you wish to opt out of all or portions of it.

Implied consent can be inferred from the relationship between the parties or from the nature of the dealings between the parties. For example, when you give Personal Information to an insurance broker or agent for the purpose of obtaining insurance, it is reasonable to infer that there is implied consent to the disclosure of that information to the insurer to meet your insurance needs.

When your Personal Information is highly sensitive, for example medical reports or financial records such as income tax returns, we obtain your express written consent in writing before using it.

Who Can Give Consent

Consent may be given by the individual or by an authorized representative (such as a person having power of attorney, or a legal guardian). Aviva will verify authorization by requesting identification, the reason for representation, and if applicable, the approval of representation by the applicable individual.

When consent is not required:

Knowledge and consent are not required in many circumstances under the law for the collection, use and disclosure of Personal Information, such as:

- Where it would compromise the availability or accuracy of the Personal Information relating to the breach of an agreement or the contravention of any law, including the detection and prevention of fraud;
- For compliance with subpoenas, search warrants, and other court or government orders;

- When Personal Information is transferred to lawyers retained by Aviva pursuant to the contractual obligation in the insurance policy to defend legal actions against the insured;
- When, under exceptional circumstances, Aviva may, under a public requirement, disclose Personal Information to appropriate authorities in matters of significant public interest;
- Where the individual is a minor, seriously ill, or mentally incapacitated, and seeking consent is impossible or inappropriate;
- Where the Personal Information is publicly available and is specified by the regulations; and
- When required by law.

Withdrawing your consent:

Subject to certain legal and contractual restrictions and reasonable notice, you may refuse or withdraw consent to the collection, use or disclosure of Personal Information at any time. But you should be aware that withdrawing your consent may affect our ability to respond to your insurance needs.

FOUR: Limiting Collection

Aviva shall only collect Personal Information that is necessary for the Identified Purposes mentioned above and such information shall be collected by fair and lawful means.

We only collect information that we need in order to do business with you. We will collect it openly, fairly and lawfully.

FIVE: Limiting use, disclosure and retention

Aviva 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. Aviva shall only retain Personal Information as long as necessary for the fulfillment of such purposes.

General

There are situations specific to the Property and Casualty insurance business where we will use, disclose and retain Personal Information as dictated by prudent insurance practices. Examples of these situations include:

- Risk sharing: transfer of Personal Information to other insurers and/or to reinsurers;
- Information services: disclosure for underwriting, claims, classification and rating purposes;
- Insurance services: disclosures to providers of goods and services to Aviva such as data processors, loss control managers, and claims adjusters; and
- Insurance intermediaries: brokers and agents.

We do not use or disclose your Personal Information for any purposes other than those previously mentioned unless we have your consent or it is required by law. We will keep your information only for as long as it is needed.

Disclosure within Aviva

Only employees with legitimate business reasons will have access to your Personal Information and must ensure that Personal Information in his or her possession is securely held.

Disclosure to Third Parties Brokers, Agents and Adjusters

Third parties, which include Brokers, Agents, Private Investigators, and Adjusters, are also subject to the Privacy Acts. Only those companies or individuals who are authorized, based on their need to carry out work for the purposes identified in Principle 2, can have Personal Information disclosed to them.

Retention Periods

The retention periods for Personal Information are consistent with the company Retention Policy, which in turn meets the provincial and federal legislation requirements.

Your Personal Information will only be retained for as long as necessary for Aviva to serve you or as long as may be required for legal purposes. As soon as any of the Personal Information reaches its maximum retention period, it is either destroyed, made anonymous, or archived from operating systems to a secured, limited access site.

Personal Information that still serves an identified purpose may be retained indefinitely provided that it is archived outside of the regular operating environment with more restrictive accessibility.

SIX: Accuracy

Aviva shall ensure that Personal Information is as accurate, complete, and up-to-date as is deemed necessary for the purposes for which it is to be used.

We will make sure to keep your Personal Information sufficiently accurate, complete, and up-to-date, to minimize the possibility that inappropriate information may be used to make a decision about you.

If Aviva has any doubt about your Personal Information being accurate, complete and/or up-to-date, given that there is a business need, we usually contact you to verify the information currently available, and process amendments where necessary.

If it is not possible to verify your Personal Information, or we are unable to contact you, no action, other than logging these limitations in your file are taken.

SEVEN: Safeguards

Aviva shall protect Personal Information by establishing and operating security safeguards appropriate to the sensitivity of the information, which is held, and to prevent any unauthorized activity relative to the information.

Responsibility for safeguarding:

Aviva is responsible for safeguarding your Personal Information from loss, theft, unauthorized access, disclosure, copying, use, or modification, regardless of the format in which it is stored. The nature of the safeguards will vary depending on the sensitivity, amount, distribution, format and method of storage of your Personal Information.

Methods of Safeguarding

The nature of the safeguards will vary depending on sensitivity, amount, distribution, format and method of storage of the Personal Information. In general, the following are observed:

- Personal Information is never left unattended out in the open;
- Access to Personal Information is only permitted when a legitimate business need exists;
- Personal Information is not photocopied, modified, disclosed, or destroyed without the specific consent and order of the responsible employee;
- When information is supplied to a third party, only necessary information is released from a sensitive file, rather than the complete file;
- No unescorted individual is given access to floors where sensitive information is retained;
- Passwords are changed on a periodic basis, and are not shared under any circumstances;
- Sensitive files are segregated and only authorized individuals allowed access;
- All mail received after hours is secured in the mail and supply area;
- Information of a sensitive nature is transferred to third parties by secure means; and
- Offsite information is stored in a secure location.

Aviva employees are required to be diligent about safeguarding Personal Information. We take particular care with sensitive Personal Information such as:

- Medical/hospital records;
- Employment records;
- Income tax return;
- Criminal records; and
- Financial records.

Information Received from Third Parties

Aviva employees adhere to the same diligence for Personal Information received from outside Aviva and adhere to any higher standard of third parties if so contracted.

Destruction of Information

All Personal Information that is no longer required for its original purpose and has been retained for the minimum required term shall be destroyed, erased, made anonymous, or archived to the secure limited access site.

EIGHT: Openness

Aviva shall make readily available to individuals on request specific information about its policies and practices relating to the management of Personal Information and complaints handling process.

Upon request, Aviva will provide an explanation of its Policy with respect to the management of Personal Information. You can contact our Privacy Officer with any inquiries or complaints or if you require further information.

NINE: Customer Access

Aviva, upon the request of an individual, shall inform them of the existence, use, and disclosure of any Personal Information about them, and they shall be given access to the information except as may be limited by law. Aviva shall amend Personal Information as deemed appropriate to ensure continued accuracy.

Requests for disclosure must be made in writing, by fax, email, or letter. We respond to all requests within 30 days.

It is important to verify that the individual requesting information is in fact the person in question. For this reason we demand that all inquiries must be in writing and that our responses, also in writing are sent to the address we have on file. Any alternative handling will require mandatory validation of the requestor's identity and address information.

Aviva will assist any individual who needs help in preparing the request.

Any responses shall be provided in an understandable manner with adequate explanation of abbreviations or codes. Upon request, Aviva will provide access to Personal Information in an alternative format for individuals with sensory disabilities, if conversion to an alternate format is reasonable and necessary.

Timeframe for Responding to the Request

Responses shall be made within 30 days of receipt of the request. However, if an extension is required, a notice of extension for up to an additional 30 days shall be sent to you, within 30 days of receipt of the request, stating the reasons for the extension, the

new time limit and explaining your right to complain to the Privacy Commissioner of Canada, or if applicable, the provincial privacy commission about the extension.

Refusal of Request for Disclosure

If a request for disclosure is denied, we will provide an explanation. The individual will be informed that he/she can challenge the denial of the request through Aviva's Privacy Officer via the Complaints Handling Process [see Principle Ten Challenging Compliance] or the Federal or Provincial Commissioner.

Examples of acceptable reasons for non-disclosure include:

- Prohibitive cost
- Personal Information that contains information about other individuals that cannot be severed
- Legal and security litigation, or commercial proprietary reasons
- Disclosure could reasonably be expected to threaten the life or security of another individual

Amending Details

If you successfully demonstrate the inaccuracy or incompleteness of Personal Information, Aviva will amend the information, as required (correction, deletion, addition). Where appropriate, the amended information shall be transmitted to applicable third parties having access to the information in question.

Maintenance of Records

All amendments resulting from this process are formally recorded with an explanation given, if necessary.

When a challenge is not resolved to the satisfaction of the individual, Aviva shall record the substance of the unresolved challenge. When appropriate, the existence of the unresolved challenge shall be transmitted to third parties having access to the information in question.

Personal Information that is the subject of a request or has been used to make a decision about an individual shall be retained as long as is necessary to allow the individual to exhaust any recourse that they may have under the applicable privacy legislation.

Cost of the Disclosure

We may charge you for providing access to your information but only after first advising you of the approximate cost.

TEN: Challenging Compliance

Aviva shall provide a means for individuals to challenge compliance with the above with Aviva's Privacy Officer.

Recognizing and Recording a Complaint or Inquiry

If you feel at any time that we are not complying with the principles set out in our Privacy Code, you may contact our Privacy Officer in writing.

For an inquiry/complaint on privacy that is received via telephone: the Privacy Officer's address information is provided along with advice to the individual to put his/her inquiry/complaint in writing to our Privacy Officer.

The Privacy Officer or designate receives all inquiries and complaints, coordinates responses, ensure responses meet Privacy requirements, and ensures that responses are timely.

Investigating

All complaints received are investigated. If we find a complaint is justified, Aviva attempts to resolve it. If necessary, we modify our policies and procedures to ensure that other individuals will not experience the same concerns.

The investigation will involve a review of the facts in order to understand your complaint by:

- Referring to the individual file (information both in the database and on paper);
- Referencing the Privacy Policy and Procedures Manual;
- Discussion with staff member(s) who were dealing with the individual/file; and
- Any other sources or documentation that may provide relevant information.

Acknowledging and Responding

If the inquiry/complaint cannot be resolved immediately, we will advise you that your inquiry/complaint is being reviewed and when you can expect an answer. If you have any concerns about our policy or treatment of your Personal Information and we have not been able to resolve it, you will be advised to contact the office of the Privacy Commissioner of Canada, or if applicable, the provincial privacy commissioner. Our Privacy Officer will provide this contact information on request.

Follow up

The Privacy Officer or designate will, if warranted and appropriate, contact you to verify whether or not the matter has been resolved satisfactorily.

If the solution means that Aviva needs to alter its practices and procedures then the Privacy Officer or designate is responsible for ensuring such changes are made.

Monitoring of Complaint Handling Procedures

On a periodic basis, the Privacy Officer or designate will review the complaints process to ensure a fair, appropriate, and prompt process is in place.

Updates to our Policy

Aviva is always considering opportunities to improve or update communication to its customers, streamline its business, but at all times be compliant with the law. Our Privacy Policy as a result, is not necessarily a static document. Aviva, therefore, reserves the right to alter the Privacy Policy from time to time. Such changes will be effective 10 days following the posting of the change on this web site. For the most up to date information, please revisit this web site or contact our Privacy Officer.

Date policy posted: January 15, 2005. Updated September 1, 2007

APPENDIX

Federal Privacy Commissioner

The Federal Privacy Commissioner's powers include:

- The right to audit an organization's information management practices where there are reasonable grounds to believe that the organization is contravening the Privacy provisions.
- The right to investigate complaints filed for contravention of a provision in Schedule 1 (the CSA Model Code) or in the body of the legislation.
- The right to issue a report in each case containing findings and recommendations
- The Act provides for fines of up to \$100,000 for interfering with the Commissioner's investigation or audit, destruction of records before a case is concluded, or where a company dismisses or disciplines an employee who whistle-blows.

How to Contact Aviva's Privacy Officer

In writing:

Privacy Officer
Aviva Canada Inc.,
2206 Eglinton Avenue East
Scarborough, ON, M1L 4S8

By Phone/Fax:

Tel: 1-800-387-4518 x54171 or 416-701-4171
Fax: 416-755-4075

By Email:

CAPrivacyOfficer@avivacanada.com

Our member companies:

- Aviva Insurance Company of Canada
- Traders General Insurance Company
- Scottish & York Insurance Co. Limited
- S&Y Insurance Company
- Elite Insurance Company
- Pilot Insurance Company
- OIS Ontario Insurance Service Limited
- Services d'Assurance Youville Inc.
- Insurance Agent Service Inc.