



Wayfarer Insurance Brokers Limited 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
How to contact Our Privacy Officer

Updated December 2010

Introduction

Wayfarer Insurance Brokers Limited (“Wayfarer”) and Elite Insurance Company are member companies of Aviva Canada Inc.¹ Wayfarer and/or Elite Insurance Company and/or Aviva Canada Inc. (“WE”) are committed to protecting and keeping private our customers’ 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.

WE and our representatives collect Personal Information for the purposes of:

- communicating with you
- underwriting and pricing your policy application and any subsequent policy changes or renewals
- servicing your ongoing insurance needs
- investigating and settling claims
- detecting and preventing fraud
- analyzing business results, compiling statistics, performing administrative tasks such as accounting and information system activities and conducting marketing and underwriting research and modeling
- reporting to regulatory or industry entities
- providing you with information on our products and services
- training employees and monitoring for quality assurance, and;
- acting as required or authorized by law

WE identify 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 our Privacy Policy.

Maurice Tulloch
President

¹ See Appendix for Aviva Canada Inc. member companies

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 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, , assets, liabilities, income, credit rating, credit and payment records, an individual's previous insurance experience, including claims history and policy 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 of 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.

Our Privacy Policy: the ten principles

The objective of our Privacy Policy is to ensure the protection of our customers' Personal Information. This includes Personal Information residing within our operations and Personal Information provided to other third parties in the conduct of commercial activities. To attain this goal, WE comply with the following principles:

- WE are responsible for Personal Information under our possession, custody, or control and a designated Privacy Officer is accountable for compliance to the Privacy Policy and Procedures. [Principle One]
- WE shall inform individuals of the purposes for which Personal Information is collected at or before the time the information is collected. [Principle Two]
- WE require 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]
- WE 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]
- WE 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. WE shall only retain Personal Information as long as necessary for the fulfillment of such purposes. [Principle Five]
- WE 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. [Principle Six]
- WE 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]
- WE shall make available to individuals upon receipt of a written request, specific information about its policies and practices relating to the management of Personal Information and its complaints handling process. [Principle Eight]
- WE shall, upon the receipt of a written request from individuals, inform them of the existence, use, and disclosure of any Personal Information about them, and they shall be given access to such information except as may be limited by law. WE shall amend Personal Information as deemed appropriate to ensure continued accuracy. [Principle Nine]
- WE shall provide a means for individuals to challenge compliance with the above with our Privacy Officer. [Principle Ten].

ONE: Accountability

WE are responsible for Personal Information under our possession, custody or control and a designated Privacy Officer is accountable for 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.

TWO: Identifying Purposes

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

WE shall collect your Personal Information from but not limited to you, government agencies, brokers, agents, insurers, other insurance reporting or data sharing agencies and credit bureaus to:

- Communicate with you
- Underwrite and price your policy application and any subsequent policy changes or renewals
- Service your insurance needs
- Investigate and settle claims
- Detect and prevent fraud
- Analyze business results, compile statistics, perform administrative tasks such as accounting and information system activities and conduct marketing and underwriting research and modeling
- Report to regulatory or industry entities
- Provide you with information on our products and services
- Train employees and monitor for quality assurance
- Act as required or as authorized by law

If WE require your Personal Information for any purpose other than as identified above, Wayfarer will seek your consent prior to using it.

THREE: Consent

WE require the knowledge and consent of the individuals 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, WE 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.

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 a 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 financial records such as income tax returns, WE obtain your express written consent in writing before using it.

In addition when you make changes to your policy or when your policy automatically renews, you are agreeing that any consent you have previously provided to us relative to your policy remains in effect unless the consent is otherwise withdrawn.

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). WE 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 us pursuant to the contractual obligation in the insurance policy to defend legal actions against the insured;
- When, under exceptional circumstances, WE 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 or permitted 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 by notifying our Privacy Officer in writing. In addition, you may also opt out of certain communications WE may send you regarding other products and services. However, you should be aware that withdrawing your consent may affect our ability to respond to your insurance needs.

FOUR: Limiting Collection

WE 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 require to do business with you. WE will collect it openly, fairly and lawfully.

FIVE: Limiting use, disclosure and retention

WE 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. WE 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 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 us such as insurance reporting or data sharing agencies, loss control managers, and claims adjusters; and
- Insurance intermediaries: brokers and agents.

WE do not use or disclose your Personal Information for purposes not identified in Principle 2 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 our member companies

Aviva Canada Inc. and/or its member companies including Wayfarer may internally share your personal information for the purposes identified in this policy with its Canadian affiliates or other related companies outside of Canada. Only such companies with legitimate business reasons will have access to your Personal Information and must ensure that Personal Information in their possession is securely held.

Disclosure to Third Parties

WE may disclose your Personal Information to: third parties, which includes brokers, agents, private investigators, and adjusters. Third Parties are also subject to PIPEDA and other applicable privacy legislation. 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.

Furthermore, should Aviva Canada Inc. and/or any of its member companies including Wayfarer become involved in any business transaction including purchase or sale, merger or amalgamation or a financing arrangement, pertaining to any of its business assets, your Personal Information may need to be shared with applicable third parties to complete such a transaction.

Disclosure Outside of Canada

Aviva Canada Inc. and/or any of its member companies including Wayfarer may use service providers located outside of Canada or related companies located outside of Canada to collect, use, disclose or store your Personal Information. Only those companies or individuals, who are authorized, based on their need to carry out work for the purposes identified in Principle 2, can perform such functions.

Where your Personal Information is collected, used, disclosed or stored outside of Canada, WE will attempt to contractually protect it, however, it may be subject to the

laws of that jurisdiction and may be accessed by the courts, law enforcement and national security services of that jurisdiction.

The jurisdictions where Personal Information may be collected, used, disclosed and stored include the United Kingdom and the United States of America. To obtain further information on our policies and practices with respect to service providers outside of Canada you may contact our Privacy Officer.

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 us 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

WE 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 WE have any doubt about your Personal Information being accurate, complete and/or up-to-date, given that there is a business need, you may be contacted to verify the information currently available, and amendments shall be made 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

WE 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:

WE are 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.

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.

Our 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 returns;
- Criminal records; and
- Financial records.

Information Received from Third Parties

Our employees adhere to the same diligence for Personal Information received from third parties 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

WE shall make available to individuals upon receipt of a written request, specific information about its policies and practices relating to the management of Personal Information and its complaints handling process.

Upon request, WE will provide an explanation of our 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

WE shall, upon the receipt of a written request from individuals, inform them of the existence, use, and disclosure of any Personal Information about them, and they shall be given access to such information except as may be limited by law. WE 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 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.

WE 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, WE 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 will 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 commissioner 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 our 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, WE 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, WE 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

WE shall provide a means for individuals to challenge compliance with the above with our 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 Policy, 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, ensures responses meet Privacy requirements, and ensures that responses are timely.

Investigating

All complaints received are investigated. If WE find a complaint is justified, WE attempt 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;
- 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 WE need 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

WE are 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. WE, therefore, reserve 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: December 2010

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.
- 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-blow.

How to Contact Our 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 are all of the subsidiaries of Aviva Canada Inc., including:

- 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.
- Wayfarer Insurance Brokers Limited
- National Home Warranty Group Inc.