



**THE PERSONAL INFORMATION PROTECTION AND
ELECTRONIC DOCUMENTS ACT
(PIPEDA)**

**PERSONAL INFORMATION POLICY
&
PROCEDURE HANDBOOK**



**Your Best Insurance
Is An Insurance Broker**

REVISED August 2004



Your Best Insurance
Is An Insurance Broker

PERSONAL INFORMATION POLICY & PROCEDURE HANDBOOK

Introduction

Property and Casualty (P&C) insurance brokers in Canada have made a commitment to respect the privacy rights of individuals by ensuring that their personal information is collected, used and disclosed in such a manner that a reasonable person would consider appropriate in the circumstances.

The federal *Personal Information Protection and Electronic Documents Act* (PIPEDA) came into force on January 1, 2001 and began to apply to certain business and activities on that date. On January 1, 2004, this Act will apply to all insurance brokerages not otherwise subject to another “substantially similar” piece of provincial legislation. This Handbook is based on the principles and rules set out in that Act.

Following the Definitions section in this Handbook, there are 10 separate policy statements, along with a series of procedural rules that accompany each policy.

Definitions

Broker — means the brokerage organization responsible for abiding by and implementing the policies and procedures in this Handbook, and includes the officers and employees of the brokerage.

Client — means an individual who engages a Broker to acquire or renew a policy of insurance.

Personal Information — means information about an identifiable individual, but does not include an employee's name, title, business address or telephone number.

Privacy Officer — means the individual or individuals appointed from time to time by the Broker to be accountable for the Broker's compliance with the policies and procedures contained in this Handbook.

© Insurance Brokers Association of Canada (IBAC), 2002. This Handbook may only be reproduced by any active member of the Insurance Brokers Association of Ontario.

Disclaimer: This Handbook is presented for general information only. Although this document is intended for public distribution, it is not intended to provide legal advice. While great care was taken to ensure the accuracy of its contents, you should seek and be guided by legal advice based on your specific circumstances.

Policy 1 -- Accountability

We are responsible for all personal information under our control and will designate one or more individuals who will be accountable for the organization's compliance with the policies and procedures described in this Handbook.

Procedures

1.1 The individual appointed to be accountable for the Broker's compliance will be known as our *Privacy Officer*. We will appoint an appropriate person in this capacity who has sufficient authority within the organization to ensure compliance.

1.2 Our Privacy Officer may be contacted as follows:

Title: Privacy Officer
Name of Organization: _____
Address: _____
Telephone: _____
Fax: _____
Email: _____

1.3 Our commitment is to:

- protect personal information;
- allow individuals to request information, seek amendments to their personal information; and file complaints against the Broker with our Privacy Officer;
- train and educate staff; and
- develop information which explains those procedures to the public.

1.4 We will use reasonable means to ensure that client personal information is given a comparable level of protection while being processed by a third party. If not practical to obtain written assurances, we may choose to make a written notation in our own file(s).

Policy 2 -- Identifying Purposes

We will identify the purposes for which we collect personal information at or before the time the information is collected.

Procedures

2.1 We will identify the purposes for which we collect personal information to affected individuals at or before the time of collection.

2.2 We may choose to identify such purposes *orally* or in *writing*. Written notification will be used whenever practical to do so. This Handbook itself may be used to identify such purposes. Common purposes for collection include:

- enabling the Broker to acquire or renew an insurance policy;
- assisting the Client and assessing his/her ongoing needs for insurance;
- assessing the Client's need for other products, such as financial products;
- ensuring that Client information is accurate and up-to-date; and
- protecting the Broker and/or insurer against inaccuracy.

2.3 We may choose to orally explain to clients the purposes for which personal information is being collected and then simply place a note in the client's file indicating that this has been done. Alternatively, an application form may be used.

2.4 We will identify any *new* purposes that arise during the course of dealing with personal information – and obtain prior consent for this new use – even if we have already identified certain *initial* purposes. However, we will only do this when the intended new purpose truly constitutes a "new" use, i.e., when the purpose now being proposed is sufficiently *different* from the purpose initially identified.

Note 1 — The *Personal Information Property/Casualty Consent* discloses the same common purposes for collection as set out in paragraph 2.3 above. If clients have received this consent form or this Handbook, we will *not provide any further disclosure* in relation to a purpose already identified by or contemplated in the form or Handbook, nor will we seek a new consent.

Note 2 — There may be situations in which we are not required to explain purposes, including those situations outlined under paragraph 3.8 "Exceptions" in *Policy 3 -- Consent*.

Policy 3 -- Consent

We will obtain the appropriate consent from individuals for the collection, use, or disclosure of their personal information, except where the law provides an exemption.

Procedures

- 3.1 We may obtain *express* consent for the collection, use, or disclosure of personal information or we may determine that consent has been *implied* by the circumstances.
- 3.2 *Express* consent is a specific authorization given by the individual to the Broker, either *orally* in *writing*. *Implied* consent is one in which the Broker has not received a specific authorization but the circumstances allow us to collect, use or disclose personal information.
- 3.3 *Express written* consent includes a client:
- signing a consent form (such as the *Personal Information Property/Casualty Consent, Personal Information Property/Casualty and Other Consent, or Personal Information Detailed Consent*);
 - providing a letter, application form or other document authorizing certain activities; and
 - providing an authorization electronically (through a computer).
- 3.4 *Express oral* consent can be given in person or over the telephone. If we obtain an *express oral* consent, we will normally make note of that consent in the client's file.
- 3.5 We will often seek *express* consent at the onset of a new business relationship. However, we may determine that by an individual seeking insurance coverage through our organization, consent has been implied for us to collect, use and disclose personal information in a reasonable manner.
- 3.6 Subject to legal exceptions, consent may be withdrawn at any time. We generally require such withdrawal to be in writing. There may be serious consequences to failing to provide or withdrawing consent, such as the Broker's inability to acquire or renew an insurance policy and/or in the cancellation of a policy.
- 3.7 Depending on whether a *new purpose* is identified during the course of dealing with a client's personal information, we may choose to seek a new consent. We do not consider a regular updating of information in a client's file to be a new purpose and, therefore, we will not seek a new consent for this purpose.
- 3.8 *Exceptions* — There are circumstances in which we are not required to obtain an individual's consent or explain purposes for the collection, use or disclosure of their personal information. These include but are not limited to:
- Collection — We may collect personal information without consent where it is in the individual's interest and timely consent is unavailable, or to investigate a breach of an agreement (such as *insurance fraud*) or a contravention of law.
 - Use — We may use personal information without consent for similar reasons as those listed beside "collection" above, and also in an emergency situation in which an individual's life, health or security is threatened.
 - Disclosure — We may disclose personal information without consent for law enforcement and national security purposes, for debt collection, to a lawyer representing our organization, and in an emergency situation in which an individual's life, health or security is threatened.

Policy 4 -- Limiting Collection

The personal information we collect will be limited to that which is necessary for the purposes we have identified.

Procedures

- 4.1 We only collect personal information for specific, legitimate purposes. We will not collect personal information indiscriminately.
- 4.2 We will only collect information by fair and lawful means and not by misleading or deceiving individuals about the purpose for which information is being collected.
- 4.3 Our policies and procedures relating to the limitations on collection of personal information will be regularly communicated to our staff members who deal with personal information.
- 4.4 The Broker may need to obtain personal information about clients *from* third parties, for example, those parties identified in the *Personal Information Property/Casualty Consent*, *Personal Information Property/Casualty and Other Consent*, or *Personal Information Detailed Consent*.

Note — There may be situations in which we collect personal information for legitimate purposes not identified to the individual, including those situations outlined under paragraph 3.8 "Exceptions" in *Policy 3 -- Consent*.

Policy 5 -- Limiting Use, Disclosure, and Retention

Personal information will 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. We will only retain personal information as long as necessary for the fulfillment of those purposes.

Procedures

- 5.1 We will only use or disclose personal information for legitimate, identified purposes.
- 5.2 We will retain personal information only as long as necessary for the fulfillment of the purposes for which it was collected. We will abide by industry standards applicable in the province(s) in which we are located, regarding minimum and maximum retention periods.
- 5.3 Personal information that has been used to make a decision about an individual will only be retained long enough to allow the individual access to the information after the decision has been made. This period will not exceed applicable industry standards.
- 5.4 Personal information that is no longer required to fulfill identified purposes will be destroyed, erased, or made anonymous. See Policy 7 -- *Safeguards*, paragraph 7.7.

Note — There may be situations in which we use, disclose or retain personal information for legitimate purposes not identified to the individual, including those situations outlined under paragraph 3.8 "Exceptions" in *Policy 3 -- Consent*.

Policy 6 -- Accuracy

The personal information we collect will be as accurate, complete and up-to-date as is necessary for the purposes for which it is to be used.

Procedures

- 6.1 Our organization will, on an ongoing basis, ensure the accuracy and completeness of personal information under our care and control.
- 6.2 Individuals who provide their personal information to us must do so in an accurate and complete manner.
- 6.3 We consider a *regular updating of client personal information* to be necessary to ensure the accuracy of client files and to provide appropriate insurance coverage for clients.
- 6.4 Our goal is to minimize the possibility that inappropriate information may be used to make a decision about any individual whose personal information we process.
- 6.5 The process for ensuring accuracy and completeness will involve:
- initial collection from client;
 - client will be asked to verify accuracy and completeness;
 - regular reviews; and
 - verifying accuracy by contacting third parties (e.g., motor vehicle and driver licensing authorities, etc.).
- 6.6 As more particularly described in *Policy 9 -- Individual Access*, we will provide recourse to individuals who appear to have legitimate corrections to make to their information on file. Once significant errors or omissions have been identified, we will correct or amend the information as appropriate. Where necessary, we will send such corrected or amended information to third parties who have had access to the information in question (such as insurance companies).

Policy 7 -- Safeguards

We will safeguard the security of personal information under our control in a manner that is appropriate to the sensitivity of the information.

Procedures

7.1 We will protect the security of personal information, regardless of the format in which it is held, against loss or theft, and against unauthorized access, disclosure, copying, use, or modification.

7.2 More sensitive information will be safeguarded by a higher level of protection. However, we will generally seek to achieve the highest level of security.

7.3 In determining what safeguards are appropriate, we will consider the following factors:

- the sensitivity of the information;
- the amount of information held;
- the parties to whom information will be disclosed;
- the format in which the information is held; and
- the way in which the information is physically stored.

7.4 When transferring client information to a third party, we will remove or mask any information that is not strictly needed by the third party.

7.5 Our methods of protection may include:

- physical measures, such as locked filing cabinets and/or restricted access;
- organizational measures, such as security clearances and limiting access on a "need-to-know" basis; and
- technological measures, such as the use of passwords and encryption.

7.6 We will ensure that our policies and procedures on safeguarding personal information are clearly communicated and accessible to our employees by:

- training staff on the subject of personal information protection; and
- having regular staff meetings in which we will review our procedures and revise where appropriate.

7.7 We will take precautions in the disposal or destruction of personal information to prevent unauthorized parties from gaining access to the information. These measures may include:

- ensuring that no one may retrieve personal information after it has been disposed of;
- shredding documents before recycling them; and
- deleting electronically stored information.

Policy 8 -- Openness

We will make readily available to individuals specific information about our policies and procedures relating to the management of personal information which is under our control.

Procedures

8.1 Individuals will be able to inquire about our policies and procedures without unreasonable effort.

8.2 We will tell our receptionist and other staff members who our Privacy Officer is so that members of the public can easily be informed.

8.3 We may choose to make information about our policies and procedures available in a variety of ways, for example:

- making this Handbook and brochures available;
- mailing out information;
- establishing a website; or
- establishing a toll-free telephone number.

8.4 The information we make publicly available will include:

- the name or title, and the address of our Privacy Officer;
- the means of gaining access to personal information held by the organization;
- a description of the type of personal information held by the organization and a general account of its use;
- written information that explains our policy and procedures (such as this Handbook); and
- a general list of the kinds of personal information made available by us to other organizations (e.g., insurance companies and other third parties). See *Personal Information Property/Casualty Consent*, *Personal Information Property/Casualty and Other Consent*, and *Personal Information Detailed Consent*.

Policy 9 -- Individual Access

Upon request, an individual will be informed of the existence, use, and disclosure of his or her personal information which is under our control, and may be given access to, and challenge the accuracy and completeness of that information.

Procedures

9.1 Upon written request, an individual will be informed as to whether or not we hold personal information about him or her. If we do hold such personal information, upon written request, we will provide access to the information, as well as a general account of its use.

9.2 The manner in which access will be given may vary, depending on the format in which the information is held (i.e., hard copy or electronic), the amount of information held and other factors. For example, if there is a large volume of information, instead of providing a copy of the entire file, we may simply provide a summary of the information.

9.3 Upon written request, we will provide a list of third parties to whom we may have disclosed an individual's personal information.

9.4 Individuals will be required to *provide sufficient information* to us to permit us to provide an account of the existence, use and disclosure of personal information.

9.5 The procedure for making a request is as follows:

- (1) All requests must be made in writing using a form such as the *Request/Complaint Form*.
- (2) We will respond to a request *within 30 days after receipt of the request*, unless we first advise you that we need a longer period to respond.
- (3) Reasons – If we refuse a request, we will inform the individual in writing of the refusal, explaining the reasons and any recourse the individual may have, including the possibility that they may file a complaint with the Privacy Commissioner of Canada.
- (4) Deemed refusal – Notwithstanding sub-paragraphs (2) and (3), if we do not respond within the above time limit, we will be deemed to have refused the request.
- (5) Costs for responding – The Broker may require payment of a modest fee to cover our administrative costs associated with preparing a response.

9.6 There are also *exceptions* which will prevent us from providing access, including where:

- personal information about another person might be revealed;
- commercially confidential information might be revealed;
- someone's life or security might be threatened;
- the information was collected without consent for the purposes related to an investigation of a breach of an agreement or contravention of the law; or
- the information was generated during the course of a formal dispute resolution process.

Policy 10 -- Challenging Compliance

An individual may address a challenge concerning compliance with the above policies and procedures to our Privacy Officer.

Procedures

- 10.1 Upon request, individuals who wish to inquire or file a complaint about the manner in which we handled their personal information – or about our personal information policies and procedures – will be informed of our applicable complaint procedures.
- 10.2 To file a complaint, an individual must fill out a *Request/Complaint Form*, which requires basic information and a description of the nature of the complaint.
- 10.3 The procedure for filing a complaint about our organization is as follows:
 - a *Request/Complaint Form* must be filed with our Privacy Officer;
 - we will acknowledge the complaint right away;
 - we will assign someone to investigate;
 - we will give the investigator unfettered access to files and personnel, etc.;
 - we will clarify facts directly with the complainant, where appropriate; and
 - we will advise the complainant in writing of the outcome of our investigation, including any steps taken to rectify the problem, if applicable.
- 10.4 We will document all complaints made by clients, as well as our actions in response to complaints, by noting these details in the individual's file and also in a master privacy file.

FOR MORE INFORMATION:

Questions on the matters addressed in this Handbook should be directed to the *Privacy Officer* of the individual insurance brokerage organization who is responsible for that organization's compliance. Contact information concerning the *Privacy Officer* may be found at page 2 of this Handbook.

Insurance Brokers Association of Ontario
90 Eglinton Avenue East, Suite 200, Toronto, Ontario M4P 2Y3
Tel: (416) 488-7422 INWATS: (888) ASK-IBAO Fax: (416) 488-7526
Web site: www.ibao.org email: contact@ibao.con.ca