

INSURANCE
BUREAU
OF CANADA



BUREAU
D'ASSURANCE
DU CANADA

Insurance Bureau of Canada

Information Privacy and You





Who we are

Insurance Bureau of Canada (IBC) is the national trade association for non-government Property and Casualty insurers in Canada and the appointed statistical agent for the government industry regulators in most of the provinces and territories. IBC is involved in a wide range of information activities: collecting data primarily from the insurance industry; processing and analyzing the data; and providing vital information to individual insurance companies, government industry regulators, and others. The processes we use in collecting, using and disclosing information have been driven, to a great extent, by the requirements of mandatory statistical plans (those statistical plans required by government industry regulators), other statutory authority and voluntary statistical plans (those plans established by agreement with voluntary participating insurers); by a variety of research programs; and by the need to support the prevention and detection of insurance fraud.

IBC ensures that information and information systems are protected regardless of the media on which the information is stored, the systems that process it, or the methods by which it is transmitted.

IBC information privacy and you

The protection of individual privacy has always been, and continues to be, a fundamental objective of IBC.

IBC has strict procedures for protecting the privacy of individuals. It collects, uses and discloses only enough personal information to serve its members and customers efficiently and fairly, while complying with federal, provincial and territorial legislation. IBC does not use or disclose personal information for reasons other than those for which the information was collected, except with the consent of the individual or as permitted by law.

What is personal information?

Personal information is information about an identifiable individual. This includes a person's name, address, and driver's licence number.



Why does IBC collect personal information?

For the most part, IBC does not deal directly with the insurance buying public. IBC collects information from insurance companies and their representatives in accordance with federal and provincial laws, statutory authority, and for the detection and prevention of insurance fraud.

One of IBC's key roles is to develop statistical reports. Personal information is summarized or rendered anonymous and these statistical reports are published, without identifying individuals, for use by:

- insurance regulators,
- actuaries in the development of various rating differentials,
- underwriters to determine the risk of exposure by classification,
- marketing and claims people to look at their market share and compare the experience of their own company to that of the industry, and
- vehicle manufacturers and the insurance industry to research vehicle safety and educate consumers.

IBC also uses or discloses personal information in order to:

- detect and prevent insurance fraud through its Investigative Services Division,
- assist insurers to properly and efficiently set premiums and settle claims,
- provide assistance and support to law enforcement agencies and other investigative bodies in their efforts to detect and prevent insurance fraud,
- track and administer programs undertaken under applicable federal, provincial or territorial legislation, and
- provide an audit trail of transfers of information between government agencies or ministries and the insurance industry as required by the government.



Can I see the personal information IBC has about me?

Yes, IBC will provide you with access to your personal information records. However, there could be some limitations to our ability to respond to your request. For example:

1. Some of the information may not be organized in a manner that makes personal information accessible.
2. In providing the information, we may delete portions that disclose personal information about other individuals.
3. If you have concerns with the accuracy of the information, we will inform you of the organization that had sent us the information so that you can ask them to correct their records. In many cases, IBC merely has custody, not ownership of the information.

How can I gain access to the personal information IBC has about me?

1. A request must be made in writing to IBC's Chief Privacy Officer (CPO), who is responsible for sending you a written response to your request within 30 days.
2. You must fully establish your identity (e.g., driver's licence, health card or other government document that contains a personal address).
3. IBC may require you to pay a fee to offset the cost of retrieving the information.

Requests are to be sent to:

Chief Privacy Officer
Insurance Bureau of Canada
151 Yonge Street, Suite 1800
Toronto, Ontario M5C 2W7
Fax: (416) 361-5952
E-mail: cpo@ibc.ca

IBC Privacy Principles



Principle 1: Accountability

IBC is responsible for the personal information under its control. The IBC Chief Privacy Officer is accountable for the organization's compliance with the principles set out in this document and all applicable provincial and federal privacy legislation.

Principle 2: Identifying Purposes

The purposes for which personal information is collected shall be identified by IBC at or before the time the information is collected.

1. IBC shall document the purposes for which personal information is collected. Identifying the purposes for which personal information is collected at or before the time of collection allows IBC to determine the information it needs to collect to fulfill these purposes.
2. 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 permitted by law, the consent of the individual is required before information can be used for that purpose.

Principle 3: Consent

The knowledge and consent of the individual are generally required for the collection, use, or disclosure of personal information. In most cases, IBC must rely on consent obtained by insurance companies.

Note: In certain circumstances personal information can be collected, used, or disclosed without the knowledge and consent of the individual. An example is information collected for the detection and prevention of fraud or for law enforcement, for which seeking the consent of the individual might defeat the purpose of collecting the information.

1. Consent is generally required for the collection of personal information and the subsequent use or disclosure of this information. In certain circumstances, consent with respect to use or disclosure may be sought after the information has been collected but before use (for example, to use information for a purpose not previously identified).

2. The principle requires "knowledge and consent". In the limited cases where IBC collects information directly from the individual, IBC shall ensure that the individual is advised of the purposes for which the information will be collected, used and disclosed.
3. IBC shall 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 fulfill the explicitly specified and legitimate purposes.
4. The method for obtaining consent may vary depending on the circumstances and the type of information collected. IBC will 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.
5. An individual may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. In that event, the individual will be informed of the consequences of such withdrawal.

Principle 4: Limiting Collection

The collection of personal information shall be limited to that which is necessary for the purposes identified by IBC. Information shall be collected by fair and lawful means.

1. Personal information shall not be collected indiscriminately. Both the amount and the type of information collected shall be limited to that which is necessary to fulfill the purposes identified.

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 allowed or required by law. Personal information shall be retained only as long as necessary for the fulfillment of those purposes.



1. Where personal information is used for a new purpose, IBC shall document this purpose. A full Privacy Impact Assessment must be undertaken.
2. In developing retention cycles, IBC shall consider both the requirements of the business and any applicable IBC corporate standards. In addition, retention cycles may be subject to legislative requirements.
3. Upon reaching its expiry date, personal information files and/or records will be destroyed, erased, or rendered anonymous. Computerized files are purged through automated system provisions. Manual repositories are usually purged through controlled and secure destruction of the records, e.g., shredding.
4. If IBC discloses information to third parties, it must track all distributions of the information. That is, who received what, when, and why, as needed.

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.

1. 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.
2. 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.

Principle 7: Safeguards

Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

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

3. Care shall be used in the disposal or destruction of personal information, in order to prevent unauthorized parties from gaining access to the information.

Principle 8: Openness

IBC shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

1. Individuals shall be able to acquire information about IBC's privacy policies and practices without unreasonable effort. This information shall be made available in a form that is generally understandable.

Principle 9: Individual Access

Upon request and where practical, an individual shall be informed of the existence, use, and disclosure of his/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. These provisions are to be applied with due regard for IBC's obligations to its members.

1. Where IBC data stores are the primary or originating source of a particular set of personal information, IBC will develop the capability required to address the following:
 - a) Provide individual access to that information, including:
 - A record search and find capability.
 - Data contents display (printout).
 - b) If the information is challenged, the record must be flagged and the challenge indicated in any subsequent use or disclosure of the information.
 - c) If the information is challenged successfully, the contents must be corrected.
 - d) If the requested change is denied and the individual pursues the matter (appeals), the record must be flagged as "under dispute" and so reported in any subsequent disclosure.
 - e) Upon final resolution, the contents should be set as "decided" and the flag removed.



2. The requested information shall be provided or made available in a form that is generally understandable. For example, if abbreviations or codes are used to record information, an explanation shall be provided.
3. IBC will provide access to an individual's personal information records. However, there could be some limitations to our ability to respond to requests.
 - Some of the information may not be organized in a manner that makes personal information accessible.
 - In providing the information, we may delete portions that disclose personal information about other individuals.
 - If individuals have concerns with the accuracy of the information, IBC will inform them of the organization that had sent the data so that the individual can request a correction from the source of the information. In many cases, IBC merely has custody, not ownership of the information.
4. IBC will provide an account of the use that has been made or is being made of personal information and to whom it has been disclosed. When it is not possible to provide a list of the organizations to which it has actually disclosed information about an individual, IBC will provide a list of organizations to which it may have disclosed information about the individual.
5. When an individual successfully demonstrates to IBC's source of the information, the inaccuracy or

incompleteness of personal information, IBC will amend the information as requested by the source. When a challenge is not resolved to the satisfaction of the individual, the substance of the unresolved challenge shall be recorded. Where appropriate, the amended information or the existence of the unresolved challenge shall be transmitted to third parties having access to the information in question.

Principle 10: Challenging Compliance

An individual shall be able to address a challenge concerning compliance with the foregoing principles to the IBC Chief Privacy Officer.

1. Procedures are in place to receive and respond to complaints or inquiries about IBC policies and practices relating to the handling of personal information. The complaint procedures are easily accessible and simple to use.
2. IBC will investigate all complaints. If a complaint is found to be justified, IBC will take appropriate measures including, if necessary, amending its policies and practices.

For more information

For more information, please write to:

Chief Privacy Officer
Insurance Bureau of Canada
151 Yonge Street, Suite 1800
Toronto, Ontario M5C 2W7
Fax: (416) 361-5952
E-mail: cpo@ibc.ca



To learn more about IBC, please see www.ibc.ca