Protection of personal information

The information contained in this procedure reflects the amendments made to the *Act respecting the protection of personal information in the private sector* (ARPPIPS) by the Act to modernize legislative provisions as regards the protection of personal information, in force as of September 22, 2023.

The purpose of this procedure is to ensure that damage insurance and claims professionals are aware of and comply with the principles set out in the *Act respecting the protection of personal information in the private sector*.

This act applies to businesses and individuals (including certified damage insurance professionals) that collect, hold, use or disclose personal information about others (s. 3.1 ARPPIPS).

In particular, every business must put in place measures, policies and procedures to protect this information and ensure that its employees understand and respect their confidentiality obligations, which apply to each stage of the life cycle of personal information: collection, communication, use, retention and destruction (s. 3.2 ARPPIPS).

For agents, brokers and claims adjusters, in order to protect your clients' personal information, it is important to develop and maintain good information protection habits, and in particular to meet the obligations related to the collection and sharing of personal information.

COLLECTION AND COMMUNICATION OF PERSONAL INFORMATION

When personal information is collected, the person concerned must be informed (s. 8 ARPPIPS):

- Of the purposes for which the information is collected and the means by which it is collected
- Of the names of third parties or categories of third parties to whom it is necessary to communicate the personal information to achieve the purposes for which it was collected
- Of their right to access and rectify their personal information
- Of their right to withdraw consent to the use or communication of the information

To offer a damage insurance product or service, a business may collect and use the client's personal information that it needs in order to offer them the products and services requested. However, the following parameters must be respected:

- The purposes for which information is collected must be clearly defined before it is collected and the client must be informed of them. For example, an agent collects personal information to assess the client's needs, determine whether they meet the insurer's underwriting criteria and prepare a quote. A claims adjuster collects personal information in order to investigate and process a claim.
- Only **necessary** information may be collected, i.e. that which is essential to achieve the purposes for which it is collected, such as placing an insurance policy or handling a claim.
- Personal information must be collected from the person concerned, unless that person has given their permission for it to be collected from a third party (i.e. another person or business). The consent of the person concerned must also be obtained before verifying their personal information with a third party.
- Particular attention must be paid to **sensitive information**, i.e. that which "due to its nature, in particular its medical, biometric or otherwise intimate nature, or the context of its use or communication, it entails a high level of reasonable expectation of privacy." In damage insurance, this includes, for example, financial or medical information.

CONSENT

Consent to the collection, communication or use of personal information must be clear, free and informed, and be given for specific purposes. In addition, it must be requested in clear, simple language. The person concerned has the right to request assistance in understanding the scope of the consent requested.

In order to comply with these requirements, any request for consent should specify the following three elements:

1. The **identity of persons or businesses** from whom the insured authorizes the collection or disclosure of personal information, for example insurers likely to accept the risk if you are a broker, or the Groupement des assureurs automobiles' Fichier central des sinistres automobiles in connection with a submission;
2. The **nature of the information** exchanged, for example, the insured's car insurance claims history; and
3. The **use** that will be made of the information collected or communicated, such as setting the insurance premium.

NB: Using a written consent form helps you to meet the statutory requirements and makes your work easier.

When the request for consent is made in writing, it must be in a document separate from the other information provided (s. 14 ARPPIPS).

EXPRESS CONSENT

In the case of sensitive personal information, consent must be obtained expressly (explicitly):

- When a business wishes to use it for purposes other than those for which it was collected (s. 12 ARPPIPS)
- When this information is to be communicated to a third party (s. 13 para. 2 ARPPIPS)

For example, sensitive personal information is collected in the context of providing a car insurance quote. If the business wishes to use this information to offer home insurance, express consent must be obtained separately.

USE OF PERSONAL INFORMATION

Personal information may only be used for the purposes for which it was obtained (s. 12 ARPPIPS). Consequently, new consent must be obtained from the person concerned before any new use or disclosure of the information collected, for example:

- When you offer home insurance to your client who already has car insurance
- If you are transferring clients to a new insurer and plan to continue with direct debits

The business must also take steps to restrict consultation of the information contained in the files, whether in paper or digital form. The business must therefore limit access by employees and suppliers to information that is necessary for the performance of their duties. For example, an accounting department employee should have access only to the information required for billing and not to the entire file (s. 20.2 ARPPIPS).

It is also recommended that non-certified employees with access to files sign a **confidentiality undertaking**, it being understood that certified employees are subject to codes of ethics and must respect the confidentiality of personal information.

RETAINING AND STORING PERSONAL INFORMATION

All necessary measures, both material and administrative, must be taken to ensure the protection and confidentiality of personal information held by the business at all times. As a certified professional, this obligation remains intact even if your mandate has ended and the person concerned is no longer your client.

Under the law and your code of ethics, you must ensure that this information is protected, regardless of where it is held or in what form it is stored. For example:

- Avoid leaving your files containing personal information in full view of the public, your office colleagues who are not concerned by these files or the residents of your home. Store them in filing cabinets (or secure computer folders).
- Use the appropriate technological tools at your disposal: confidential passwords, data encryption systems, firewalls, etc.
- Make sure that your home workstation is not located in an open area where your confidential business telephone conversations could be overheard.

A PERSON IN CHARGE OF THE PROTECTION OF PERSONAL INFORMATION AND AN INCIDENT REGISTER

As of September 22, 2022, businesses are required to appoint a person in charge of the protection of personal information within their organization. In many cases, the person in question is a senior executive (s. 3.1 ARPPIPS). This person ensures that the business handles the personal data it holds in accordance with the law. In particular, the person must manage confidentiality incidents.

As a certified professional, it is your responsibility to know who is the person or department responsible for protecting personal information within your business. In the event of a confidentiality incident, you must contact this person or the department responsible to:

- Report any confidentiality incident in which you are involved
- Take reasonable steps to reduce the risk of harm to the persons concerned and to prevent further incidents of a similar nature

Examples of confidentiality incidents:

- Sending an email containing personal information to the wrong recipient
- Theft of a laptop containing clients' personal information
- Hacking leading to theft or loss of data
- Extraction of data by an unauthorized person

DESTRUCTION OF PERSONAL INFORMATION

Businesses must keep their files in their entirety until five years after the last transaction involving them.

Then, files kept on paper or digital media must be securely destroyed to preserve their confidentiality.

If you entrust the destruction of your files to a specialized company, make sure that your contract contains a confidentiality undertaking and require it to be signed by anyone who will handle your documents.

EXERCISE OF THE RIGHT OF ACCESS TO PERSONAL INFORMATION BY THE PERSON CONCERNED AND RELATED PROCEDURES

Subject to certain exceptions, all individuals have the right to access personal information about them held by a business (s. 27 ARPPIPS). They also have the right to request rectification of inaccurate, incomplete or equivocal personal information or information whose collection, communication or retention is not authorized by law (s. 28 ARPPIPS). All requests for access must be made in writing (s. 30 ARPPIPS) and processed within 30 days of receipt by the person responsible for personal information (s. 32 ARPPIPS).

To learn more about the content of a client file, see the procedure "*Tenue de dossiers clients et notes aux dossiers*" (available in French only).