Privacy policy and Breach Procedure

Bourne Financial Bourne Inc.

Chief privacy officer: Andrew Bourne

Date of revision: October 1st, 2023

Table of contents

1. Our Commitment

To give you access to financial products and services, we collect some of your personal information and ensure its protection. We comply with the Personal Information Protection and Electronic Documents Act (PIPEDA), a federal law protecting personal information, and any applicable provincial laws. We also base this policy on the recommendations and code of ethics of the Chambre de la sécurité financière, the self-regulatory organization for our industry. Please refer to Appendix B for references to the code of ethics and frequently asked questions.

2. Responsibility

We are responsible for the personal information we receive from our clients. We shall protect this information regardless of how it was transmitted.

3. Consent

We will only collect the information with your consent. Your personal information will be used to find financial products, concepts, and services that meet your identified needs. By signing the consent form, you agree, on behalf of yourself, your executors, administrators, or assignees, to:

- Provide accurate information throughout our business relationship and as your situation evolves.

- Allow us to use, transmit and disclose this information if needed to our suppliers, associates, and managing general agents, that may preserve some of this information in their files for future use or recommendation from us, our suppliers, and any assignee.

- Allow us to preserve your personal information, including medical information that may appear on your proposals, in our physical or electronic files for as long as you wish to do business with us or we have a business or regulatory need to preserve the information.

- Assign your file, including your personal information, to another agent and/or MGA to continue to serve your needs in the event of disability, death, retirement, or any other major event that may affect our firm. However, you have the right to choose your agent at that time should you disagree with the one being assigned to you.

4. Reasons for collection/use/preservation

We collect all the personal information (including medical, financial, and company-related information) with your consent. We use and maintain it solely to provide advice, administer products or services you purchase through us, and recommend new products and services that may interest you.

5. Limits of collection

We only collect and preserve information that helps us advise you, including personal, financial, and medical information, and allows us to meet our regulatory obligations. We only use fair and lawful means to collect this information.

6. Limits of use/transmission/preservation

We will use and disclose your personal information to fulfill our duties, advise you, and, when appropriate, comply with the law. The personal information contained in your client file will only be disclosed to:

- Our employees and staff that we will have authorized, for example, professionals that could help you in areas of expertise beyond our competence.
- Companies whose products and services we offer and their employees and representatives in their effort or attempt to provide you financial products and services or any other related activity (and for any other purpose you have authorized).
- Selected third-party service suppliers that we have authorized; if they are located outside of Canada, your personal information may be subject to the applicable laws, including access to information laws of public authorities, of other countries.
- Individuals or entities to whom you have authorized access by law.

We must preserve most of the information we collect for regulatory reasons, including the requirement to demonstrate that the recommendations that we make are appropriate and meet your identified needs.

By applicable laws and your written authorization, you have the right to review the personal information contained in your file. At your request, copies (not originals) of other personal documents, such as insurance policies, wills, or mandates (proxies), could be kept in your file.

7. Information Accuracy

To make the appropriate recommendations, we must receive accurate information. It is our responsibility to keep your information as accurate and up-to-date as possible. When possible, we will try to update your personal information to determine whether the recommendations that we made are still appropriate as your situation evolves. However, we need you to provide us with regular updates for the same reason. You can review the personal information we keep about you upon request.

8. Efforts to protect your personal information

All staff, associate advisors, managing general agents, and suppliers who have access to the client files must protect this information, keep it confidential and use it solely for its intended purposes. The information no longer required for the intended purpose will be destroyed. We also implemented physical and computer safeguards, and other processes, to protect client information from unauthorized access. Following the PIPEDA recommendations, all new employees sign a confidentiality agreement, and we make sure to raise awareness by following trainings and reading contents on a regular basis about the importance and impact of sensible data protection and cybersecurity.

Under Appendix A, we enclose our procedure in the event of a default, breach, or violation of the protection of your personal information.

9. Your right regarding personal information

You can withdraw your consent at any time (subject to contractual or legal restrictions to provide us with reasonable notice) by contacting us. Should you withdraw your consent, we could be unable to provide you with the requested products or services, and we may have to terminate our business relationship.

10. Your right to file a complaint

Should you have any concerns regarding the collection, use, or disclosure of your personal information, you have the right to file a complaint with us or with the Office of the Privacy Commissioner.

Privacy Commissioner:

Bourne Financial Group Inc.
Att: Andrew Bourne
297 Ch. Du Bord du Lac Lakeshore, Unit 201
Pointe-Claire, Quebec
H9S 4L4
514-489-6666
abourne@bournefinancialgroup.ca

Office of the Privacy Commissioner of Canada
30, Victoria Street
Gatineau (Québec) K1A 1H3
Toll-free: 1-800-282-1376

APPENDIX A – Procedure in case of default/breach/violation

A privacy breach occurs when there is unauthorized access to personal information or unauthorized collection, use, or disclosure of such information. Those activities are "unauthorized" when they violate applicable privacy laws such as the Personal Information Protection and Electronic Documents Act (PIPEDA) or similar provincial privacy laws. Some of the most common privacy breaches occur when a consumer, patient, client, or employee's personal information is stolen, lost, or mistakenly distributed (e.g., the theft of a computer containing personal information or mistakenly sending an email containing personal information to the wrong person). A breach may also be the result of a procedural or operational failure.

As determined by the Commission d'accès à l'information du Québec (www.cai.gouv.qc.ca/english/), we will follow the (6) following steps in the event of a privacy breach:

1) Produce an incident report
2) Make a preliminary assessment of the situation.
3) Limit the invasion of privacy.
4) Assess the risks associated with the breach.
5) Notify the concerned individuals.
6) Prevent.
7) Follow up.

Step 1 : Produce an incident report

We will complete an incident report with the following information and send it to the Quebec Commission d'accès à l'information:

Date
Name
Location and date of incident
Description of the incident
Cause (if known)
People affected by the incident (client, employee, advisor, third party)
Type of personal data impacted
Brief description of actions to circumscribe the breach
List of people who were informed and when
Additionnal comments

Step 2: Make a preliminary assessment of the situation

a) Briefly define the context of the loss or theft of personal information:
   - Identify the affected personal information and its support.
   - Identify the individuals, their number, and the group of individuals (clients, employees, etc.) affected.

- Establish the context of the incidents (date, time, location, etc.).
- Identify, if possible, the circumstances of the loss (cause, individuals likely to be involved in the incident, etc.).
- List the physical and IT security measures in place at the time of the incident.

b) Inform the relevant external authorities who must be notified of the incident immediately: (before the risk assessment)
   - Police department (if the circumstances suggest the possibility of a crime).
   - Commission d'accès à l'information (form here)

c) Assign an individual or team responsible for handling the situation.

d) Inform internal stakeholders:
   - The management team of the organization or company
   - The head of the relevant administrative team
   - The Privacy Commissioner
   - The Legal counsel
   - The Communications Department (media and customer call management)

Step 3: Limit the invasion of privacy

Take prompt and appropriate steps to limit the consequences on the affected individuals of the potential wrongful use of their personal information or usurpation or theft of their identity:

a) Take immediate steps to limit the consequences of the loss or theft of personal information to ensure that the illegal practice is stopped if needed.

b) Recover the physical or digital files, if applicable.

c) Revoke or change passwords or computer access codes.

d) Check for gaps in security systems.

Step 4: Assess the risks associated with the breach

a) Fill in a preliminary risk assessment while considering the sensitivity of the personal information at issue, its nature, quantity, the possibility of combining it with other information, the individuals involved, etc.

b) Determine the context of the incident, including:
   - The cause (e.g., a deliberate or inadvertent loss or theft of personal information, human error, computer failure, etc.)
   - The known or likely perpetrators of lost or stolen personal information (e.g., criminal organizations, the general public, etc.)
   - The extent of the situation (number of individuals and areas affected)
   - The possible systemic nature of the theft of personal information (especially if the loss was not the direct result of human intervention)
   - An assessment of the likelihood of a similar incident occurring again.

c) Assess the possibility of the affected personal information being used in a manner that is harmful to the individuals concerned, considering, among other things, the security measures taken to protect it, the difficulty of accessing it, and its intelligibility (password, encryption, etc.).

d) Assess the reversibility of the situation, including the possibility of recovering the lost personal information.

e) Assess whether the immediate measures taken were appropriate to limit the breach and complete them if necessary.

f) Determine potential harm, including assessing the possible use of personal information by malicious individuals, notably for identity theft.

g) Determine priorities and identify the actions to be taken based on the results of these risk assessments.

Step 5: Notify the concerned individuals

a) Determine who should be informed of the loss or theft of personal information based on the risk assessment:
   - Police department: if the loss may result from a crime, the concerned police department must first be aware of the elements surrounding the loss and then of the subsequent actions taken. It is essential not to interfere with the investigation and to preserve potentially relevant evidence.
   - Concerned individuals: if the loss or theft of personal information poses a risk of harm to concerned individuals, they should be notified immediately. This is not to alarm them but to allow them to take appropriate actions to protect their personal information.
   - Commission d'accès à l'information: if the individuals affected by the personal information are from Québec, the Commission could initiate an inspection or investigation and play an advisory role in the search for a solution.
   - Others: other parties may need to be notified, such as credit agencies, agents, government bodies, unions, professional orders, etc.

   However, in disclosing the loss of personal information, special care must be taken not to exacerbate the harm that may be caused to the individuals concerned (e.g., keep personal information in notices to a minimum).

b) Assign individuals responsible for notifying the previously identified external stakeholders and the time and means of communication (letter, email, phone, etc.).

c) If applicable, identify and record the reasons for the decision to not notify the individuals affected and other stakeholders.

Notice to individuals affected by a loss or theft of personal information

Depending on the circumstances, individuals may need to be notified of the loss or theft of their personal information. This notice may include some of the following:

- The context of the incident and the moment when it took place as well as a description of the nature of the personal information affected or potentially affected, without disclosing specific personal information
- A brief description of the actions taken to limit or prevent any harm and a list of individuals who have been notified of the situation (Police Department, Commission d'accès à l'information, etc.)

- The organizations and companies' actions to help the affected individuals (Help and Information service, credit monitoring subscription, etc.)
- Actions that the affected individuals can take to reduce the risk of harm or to protect themselves better (reference to the document "Le vol d'identité" available on the Web site of the Commission d'accès à l'information)
- Other general information materials designed to help individuals protect themselves from identity theft
- The contact information of an individual within the organization who could answer questions and to whom any reports can be made
- Key actions that will be taken to prevent the situation from happening again (change in practice or process, staff training, review or development of policies, audits, periodic monitoring, etc.)

Step 6: Prevent

a) Further analyze the circumstances of the loss or theft of personal information and provide a chronological description of the events and actions taken following this incident, including dates and concerned parties.

b) Identify and review internal standards, policies, or guidelines in place at the time of the incident, regarding computer security, when information is involved, and privacy in general.

c) Check if these internal standards, policies, or guidelines have been followed by the individuals involved, and identify why they have not, if applicable.

d) If it was a procedural error or operational failure, document it in the safety record and adjust procedures to prevent the incident from occurring again.

e) Assess the need to develop a policy for handling lost or stolen information within the organization or company.

f) Formulate recommendations for medium and long-term solutions and prevention strategies.

g) Assess whether the collection of personal information is necessary for the organization or company.

h) Determine the necessary follow-up.

Step 7: Follow up

It is essential to follow up on:

a) The handling process that must be applied in the event of a loss or theft of personal information and on the results obtained in order to improve it, if applicable.

b) The safety measures required as a result of the incident and their performance in order to improve the process in place and update the privacy policy.

c) The communication of relevant information to the Commission d'accès à l'information and the involved police department, if applicable.

Record-keeping

You are also required to keep a record of all incidents related to the breach of personal information, even when there is no risk of serious harm. All incidents must be kept on file for at least two years so that the Office of the Privacy Commissioner can review them upon request.

The records must include, at a minimum, the following:

- The date or estimated duration of the breach
- A description of the circumstances of the breach
- The nature of the information involved in the breach
- The filing of a report to the Office of the Privacy Commissioner or the names of other organizations that were made aware, if applicable
- A brief explanation of why the organization determined there was no risk of serious harm if the breach was not reported to the Office of the Privacy Commissioner

Resources

Detailed information on all your privacy obligations can be found at www.priv.gc.ca.

APPENDIX B – References from the Chambre de la sécurité financière

Code of Ethics

A representative must ensure that the information he obtained about his clients remains confidential unless certain legal provisions or a court order allow him to disclose it. He is also required to use the information he obtained for the purpose for which it was obtained and not use it to the detriment of his client.

Sections 26 and 27 of the Code of Ethics of the Chambre de la sécurité financière provide these obligations.

Section 26 – A representative must respect the secrecy of any personal information that he obtains about a client and only use that information for the purposes for which it was obtained unless he is relieved of that obligation by a provision of a law or by order of a competent court.

Section 27 – A representative must not disclose personal or confidential information that he obtained, except in accordance with the provisions of the Act, and must not use that information to the detriment of his client or to obtain an advantage for himself or for another person.

Please also note that section 23 of the Act respecting the distribution of financial products and services provides that a representative must submit all the information he collects about his clients to the institution he is affiliated with. He can only disclose the information to an individual authorized by law to receive it.

Frequently asked questions

Q: Do the files and records kept need to be stored in a locked filing cabinet and a locked room?

R: In general, records need to be kept in a safe and secure location. This location should not be easily accessible to people other than those authorized. Of course, it is important to ensure that the records can be retrieved promptly and easily when a duly authorized individual wishes to access them. Thus, keeping records in a locked filing cabinet inside a locked room is a good way to meet these obligations. However, any other safe method of achieving the same objective would be equally acceptable.

Q: What about the preservation of electronic records?

R: For electronic records, the same rule applies as for physical records, in that they need to be kept in a safe and secure manner.

Q: Should we use a separate filing cabinet for each type of record or file kept?

R: One of the main principles in record-keeping is that records must be kept so they can be recovered promptly. This requires using an effective filing system that allows each type of file or record to be retrieved. Using a separate filing cabinet for each type of file, combined with appropriate codification, could be effective, although it is not required.

Q: In a client file, do we need to include a detailed description of the contract sold even when a copy of the proposal and an illustration of the products sold are enclosed with the file?

R: What matters in record-keeping is that the information required by the Regulation respecting the keeping and preservation of books and registers be found in your files. Moreover, do not forget that these files will allow you to provide a professional service to your clients. The goal of these files should be easy access to all the information you need to advise your clients properly. Your client files should include the following information: your client's contact details (name, date of birth, address, telephone number, fax number, and email address), subject, nature and cost of the product sold or service rendered, the policy number, the date of issuance of the contract and the signature of the proposal or service request, the name of the representative involved in the transaction, their method of payment, and that, for each product sold and service rendered, the date and method of payment of the product sold and service rendered, a copy of the Financial Needs Analysis (FNA) of the client, a copy of the form required for the replacement of a policy as well as any other information collected from the client, and any related documents. Thus, when the copy of the proposal and the product illustration contain all the above information, you are not required to detail the contract sold. However, you can very well add more information than required as long as it is relevant. Furthermore, ensure you meet the record-keeping requirements imposed by the institution you are affiliated with.

Q: If an individual is the only life and health insurance representative in their firm, what regulations must they follow?

R: According to the provisions of the Act respecting the distribution of financial products and services, the Regulation respecting the keeping and preservation of books and registers, and the Regulation respecting firms, independent representatives, and independent partnerships, you must apply the rules according to the type of practice under which you operate. In practice, for a representative to obtain a right to practice, they must hold a certificate issued by the AMF as well as professional insurance and must be authorized to practice under a particular mode of practice, in accordance with section 14 of the Act respecting the distribution of financial products and services. Therefore, it is this practice mode you must refer to. Thus, if you are an independent representative and are not affiliated with a firm or an independent partnership, you must apply the rules governing independent representatives. On the other hand, if you carry out your activities for a firm or an independent partnership, you must apply the regulations imposed on them.

Q: Can a financial security advisor keep a copy of all the insurance proposals submitted during the review of a file?

R: No law or regulation prohibits the representative from keeping insurance proposals in the client file if the information is relevant. In fact, the Regulation respecting the keeping and preservation of books and registers provides for all the useful and required information collected from the client and all related documents to be preserved on file. Furthermore, your ethical obligations stipulate that you must be in full knowledge of the facts. Therefore, it would be logical to keep this information on file.