COMPLIANCE PROGRAM FOR PRIVACY

Required under Personal information protection and electronic documents Act (PIPEDA) or applicable provincial privacy legislation

CONTE FINANCIAL SERVICES INC.

Compliance Officer: Tony Conte and/or Josee Veitch

Effective: December 31, 2015
Revised on:

1. Privacy and our business

Clients provide us with personal information that is essential to our business and protecting this information is important to maintaining their trust and confidence. The federal privacy law, the Personal Information Protection and Electronic Documents Act (PIPEDA), governs the collection, use and disclosure of personal information. Personal information is defined as any information about an identifiable person (including health and financial information), with the exception of the person's name, business address and business phone number where the person is an employee of an organization.

We are responsible for taking appropriate steps to safeguard the personal and confidential information in our possession. In some situations, this will mean we must adopt new business practices to safeguard personal information.

We abide by the Insurance Company suppliers' that we use, privacy guidelines, which are based on principles recognized in PIPEDA.

2. Concerns and general requests

Any concerns or general requests related to privacy and Conte Financial Services Inc. services are to be made in writing and sent to:

Conte Financial Services Inc.:

Tony Conte or, Josee Veitch
205-460 West Hunt Club Rd
Ottawa ON K2E 0B8

The CFS compliance officers can also be reached by email at:

tconte@cfservices.ca
jveitch@cfservices.ca

Any concerns or general requests related to privacy and any insurance company suppliers' products and services are to be made in writing and sent to the Chief Compliance officer for that company. The contact information for any supplier that we use can be obtained either by visiting the web site for that specific company or by contact the compliance officer for CFS who will provide it.

Client requests for personal information

Under PIPEDA, clients have the right to request information about them held in files maintained by either us or any insurance company.

A client can request copies of their personal information held by CFS by writing to the Compliance officer(s) for CFS.

Given that each insurance company or supplier has their own specific process, should a client wish a copy of their personal information held by an insurance company or other supplier, they should contact the CFS compliance officer for instructions. The request can also be made through the CFS advisor who will notify the CFS compliance officer.

Misuse of personal information:

Any misuse of personal information relating to products and services provided by CFS should be reported immediately to the chief compliance officer(s). Should any misuse of personal information relating to products and services provided by any supplier, the CFS advisor will advise the CFS Compliance officer(s) who will advise the Chief Compliance officer for that specific supplier.

3. Collection of personal information:

We only collect personal information that is necessary for the purposes indentified.

We take reasonable efforts to ensure client and prospect information held in client files is accurate and is updated or corrected as needed.

We take appropriate measures to ensure that information we've collected is used for the purposes identified and that it is not used for another purpose or disclosed to a third party without the client's or prospect's consent, except as may otherwise be allowed by law.

Recording client telephone calls

Any recording of client calls involves the collection of personal information therefore the practice must meet fair information practices. The same rules apply to calls initiated by the client and to calls initiated by the advisor.

- We can only record calls for specified purposes;
- The individual must be informed that the conversation is being recorded at the beginning of the call and we must make a reasonable effort to ensure the individual is advised as to the purposes for which the information will be used;
- Recording may only take place with the individual’s consent. If the caller objects to the recording, we should provide the caller with meaningful alternatives;
- The information collected must only be used for the specified purposes; and
- We must ensure that we comply with the other provisions of the Act with respect to matters such as safeguards, access, retention and disposal.
- If a client requests access to their information in our files, it is conceivable that we will have to provide the recording or transcription of the recording of calls with the client.

4. Use, disclosure and retention:

Personal information that is no longer required to fulfill the purpose(s) identified when it was collected is destroyed or erased. If we believe we have a need to keep any additional information we have the client sign the appropriate area of the authorization form allowing us to retain this material.

We are solely responsible for the safe keeping of this material, for maintaining its confidentiality and for its return to the client.

When paper materials containing any client or prospect personal information are to be destroyed, this should be done by shredding, not recycling.

5. Safeguards

Appropriate safeguards must be taken in the storage and disposal of client information. When information is no longer required we dispose of client information by shredding paper and ensuring all information has been deleted from end user devices including personal computer (desktop or laptop), consumer device (e.g., personal digital assistant (PDA), smart phone), or removable storage media (e.g., USB flash drive, memory card, external hard drive, writeable CD or DVD) that can store information. Storage devices must be destroyed when being disposed of to ensure the information is not retrievable.

We take appropriate precautions to safeguard client information from third parties who may have access to the premises, i.e., security, cleaning services and suppliers.

6. Consent

When collecting information from clients and prospects, we must be prepared to explain the purposes behind why we are collecting this information. While client consent to our collection and use of personal information does not necessarily need to be stated directly or in writing, we provide information to a client or prospect about our own privacy practices. This information can be given verbally to clients or provided on paper at an initial meeting. In keeping with good client file practices, we document in the client's file that this information was reviewed with the client or prospect.

We only disclose personal information about clients to another person or company if we have the verbal or written consent of the client, or if we are otherwise allowed or required to do so by law. We can recommend other professionals or advisors to clients if they ask us or if we believe they may benefit from such services. We never provide any client names or other information to third parties who may use it to market their services unless we have the client's consent.

Steps to obtaining client consent

- We obtain consent from all clients for new access to their information. This includes sales of business to another advisor or providing access to a new administrative support person (excluding employees of suppliers we use). The consent requirement can be handled a number of ways - by telephone, fax, email, letter, newsletter or a personal visit.
- If we send a letter, the letter should name the new advisor and contain a contact name and number for the current advisor, in case the client, on receiving the letter, objects to the transfer of his or her information or to its access by another advisor.
- If a client objects to this transfer or new access, depending on the situation, the client has the right to:
    - Request that his/her information not be disclosed to the new advisor
    - Request a new advisor
- The new advisor should not use or access information in the client file until consent is obtained. We will allow 20 business days for the client to voice an objection, after which time it can be assumed consent has been obtained.
- The new advisor is responsible for handling the file/information appropriately going forward.

Agent of Record (AOR) changes

Since clients initiate AOR transfers, we can assume that we have implied consent to transfer access to their information and their files (or a copy of their files), if applicable to the new advisor. Therefore, there's no need to have official consent included along with instructions from the client.