EXPERIOR FINANCIAL GROUP INC.

PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT (PIPEDA)

POLICIES AND PROCEDURES

Privacy Compliance Officer: Connor Moseley

- 660 Speedvale Ave West, Suite 205
- Guelph, ON
- N1K 1E5
- 519-826-0770

Program Effective: March 26 2014
Program Update: March 2020

Table of Contents

Our Commitment

In order to provide Agents and their customers with access to insurance products and services, we collect certain personal information about both, generally on behalf of our insurance providers. Our commitment goes beyond meeting legal requirements for protecting personal information. The trust and confidence that our Agents and insurers hold in us, including our ability to protect the confidentiality of personal information and the privacy of the individuals who provide it, are critical to our success as a business. This Policy applies to our employees and any third-party service providers or representatives with which we contract.

What is Personal Information?

"Personal information" means any factual or subjective information concerning an identifiable individual. Personal information may be collected concerning a variety of individuals with whom our company does business, including from group and individual life insured, beneficiaries, employees, agents, and insurance companies.

Examples of personal information include:

- information concerning an individual's name, age, sex, health, personal characteristics or personal and financial circumstances.
- opinions, evaluations, comments, social status, or disciplinary actions;
- employee files, credit records, loan records, medical records, existence of a dispute between a consumer and a merchant, intentions
- Personal information can also include such things as identification numbers (such as SIN or employee numbers), banking and income information, employment records, credit records and medical information.

Personal information can be collected in a variety of forms, including written (such as correspondence and memoranda) as well as electronic communications and records, video or audio recordings and photographs.

Personal information **does not** include the name, title or business address, telephone number or e-mail address of employees of an organization.

PIPEDA's 10 Principles – Our Responsibilities and How We Comply

PIPEDEA incorporates the 10 principles of Canadian Standards Association's Model Code for the Protection of Personal Information and imposes certain responsibilities on insurers and MGAs operating on their behalf regarding how they handle customers' and Agents' Personal Information in their possession. Our Privacy Policy is designed for Agents, so that they understand how we manage their Personal Information as well as that of their customers

Principle 1 - Accountability:

Requirement: *Appoint an individual to be responsible for our MGA's compliance*

How We Comply: Experior Financial Group, its employees and contractors are responsible for all personal information in their possession or control, including information that has been obtained from or transferred to a third party for processing.

Experior has appointed Connor Moseley as the Compliance Officer. He is responsible for ensuring that Experior and its agents follow industry standards set out by law and provincial regulators.

To ensure privacy, Experior does not outsource our processing to any 3rd party.

Experior conducts its business in accordance with PIPEDA in Canada, ALPIPA in Alberta, BCPIPA in British Columbia, and ARPPIPS in Quebec.

Principle 2 - Identify Purposes for Collection:

Requirements: *identify the reasons for collecting personal information before or at the time of collection.*

How We Comply: Experior collects personal information in a number of ways, for example through interview, applications/agreements or other means. Prior to or at time of collection Experior identifies the purpose of the collection which is communicated when possible in writing. Depending on the manner in which the information is being collected it may also be done orally.
We collect only the information we need to fulfill our contracts with Agents and Insurers, commission purposes, and to meet regulatory obligations. We will only use fair and lawful means to collect this information.
Experior will not collect, use, or disclose the information beyond that which is required to fulfill the purposes specified at the time of collection. Unless it is required by law, any collection of personal information for a previously undisclosed purpose will identify the new purpose and obtain the consent of the agent.
Experior never collects personal information directly from customers.

Persons collecting personal information are expected to be able to explain to individuals the purpose for which the information is being collected.

Principle 3 - Consent:

Requirements: *Obtain the individual's consent before or at the time of collection, and when a new use is identified.*

How We Comply: Experior will obtain valid consent for the use or disclosure of personal information at the time of collection. The consent can be express or implied. We will usually seek express consent when the personal information is likely to be considered sensitive. Sometimes, consent will be obtained after the information has been collected but prior to use (for example, when the company wishes to use

information for a purpose not previously identified).
Implied consent may be inferred in circumstances where the information is less sensitive and consent to collection, use or disclosure can be reasonably inferred.
Sometimes consent may be obtained from an authorized representative, such as a legal guardian or person holding a power of attorney.
In certain limited circumstances, PIPEDA has outlined when personal information can be collected, used, or disclosed without the knowledge and consent of the individual:

if it is clearly in the individual's interests and consent is not available in a timely way;

- if knowledge and consent would compromise the availability or accuracy of the information and collection is required to investigate a breach of an agreement or contravention of a federal or provincial law;
- if it is publicly available as specified in the regulations;
- when it is contained in a witness statement and the collection is necessary to assess, process, or settle an insurance claim;
- where it is produced by individuals in the course of their employment, business or profession– as long as the collection is consistent with the purpose for which the information was produced;
- When information is being collected for the investigation of a potential breach of contract, the prevention or detection of fraud or for law enforcement purposes, seeking the consent of the individual might defeat the purpose of collecting the information.

An individual may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. Experior will inform the individual of the implications of such withdrawal, which may include termination of a policy, termination of benefits or inability to process a claim.

Principle 4 - Limit Collection of Information:

Requirements: *collection of personal information will be limited to that which is reasonably necessary for the identified purposes. Information shall be collected only by fair and lawful means.*

How We Comply: Experior does not collect personal information indiscriminately. Both the amount and the type of information collected shall be limited to that which is reasonably necessary to fulfil the purposes identified.
Information will be collected in a manner that complies with the company's obligations to identify the purpose of collection and to obtain the consent of the individual to collection, use and disclosure of personal information.
For example: we only collect customer information required to issue a policy or to create a file that allows the Agent to demonstrate the appropriateness of the sale. We collect Agent information required to screen for suitability, and fit with the organization, contracting with insurance carriers, commissions purposes and any information needed to meet regulatory requirements.

Principle 5 - Use, Disclosure, Retention:

Requirements: *Do not Use or disclose personal information only for the purpose for which it was collected, unless the individual consents, or the use or disclosure is authorized by the Act. Keep personal information only as long as it is needed to satisfy the stated purposes.*

How We Comply: We collect, use and retain personal information from individuals in order to perform our functions as stated in our Privacy Policy. We look to insurers to inform us of their record retention requirements for customer information. Personal information that has been used to make a decision about an individual will be retained long enough to allow the individual access to the information after the decision has been made. Personal information that is no longer required to fulfill its purpose shall be destroyed.

Principle 6 - Accuracy:

Requirement: *Minimize the possibility of using incorrect information when making a decision about the individual or when disclosing information to 3rd parties.*

How We Comply: The extent to which personal information shall be updated will depend upon the use of the information, taking into account the interests of the individual. Information will 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.
We vet insurance applications and forms on behalf of insurers, in order to be able to submit agent business that is to ensure that the information provided to insurers is complete and accurate.
Experior Financial Group will not routinely update personal information, unless such a process is necessary to fulfil the purposes for which the information was collected.

Principle 7 - Safeguards:

Requirements: *Protect personal information from unauthorized access, disclosure copying or use, and against loss or theft.*

How We Comply: Experior Financial Group has implemented security safeguards and appropriate training to protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use or modification.
Security safeguards vary depending on the nature and format of the information collected. The methods of protection include physical, organizational and technological measures designed to limit access to authorized persons, ensure the integrity of the information and protect it from unauthorized use or disclosure.
Security safeguards also include steps to ensure that all third parties with whom we contract and who may be required to handle personal information have implemented comparable security measures.

Principle 8 - Openness:

Requirements: *Make privacy policies and procedures understandable and readily available.*

How We Comply: our Privacy Policy is provided to Agents is posted on our website and always available. It can also be provided upon request.
For a detailed list of safeguards used to protect private information please see Appendix A.

Principle 9 - Individual Access:

Requirements: Upon request, an individual will be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual will be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

How We Comply: Upon request, Experior will inform an individual: whether or not it holds personal information about the individual, we will permit the individual access to the information, and account for its use.
All requests will be responded to within a reasonable time frame and at no cost to the individual.
For more information on access to personal information see Appendix B.

Principle 10 - Provide Recourse:

Requirements: *Inform complainants of their avenues of recourse. These include our MGA's own complaint procedures, those of industry associations, regulatory bodies and the Office of the Privacy Commissioner of Canada.*

How We Comply: Experior Financial Group will inform individuals who make inquiries or lodge complaints of the applicable complaint handling protocol.
Experior will investigate and respond to all complaints in accordance with the applicable departmental complaint handling protocol. If a complaint is found to be justified, Experior Financial Group will take appropriate measures, including if necessary, amending its policies.
For further information on the recourse available please see Appendix C.

Contact Us: If you have any questions or concerns regarding this Policy or how we manage your personal information, please contact our Privacy Compliance Officer. Please note that a complaint should be directed in writing. We will not respond to complaints via email.

Name _____
Address _____
Phone _____
Fax _____
Email _____

Appendix A

Safeguarding information

How we safeguard PERSONAL INFORMATION is very likely the most critical element of our privacy efforts, given the sensitive nature of information that we collect directly and indirectly, which we use and retain.

We must have appropriate safeguards to ensure that PERSONAL INFORMATION is protected from loss, theft and inadvertent destruction, among other things.

PERSONAL INFORMATION owned by Agents, employees and customers is maintained in paper and electronic format in our offices. We have the following controls in place to safeguard this information:

Physical Safeguards – we ensure that our premises are secure through use of

- Locks
- Fire suppression
- Our paper files holding PERSONAL INFORMATION are kept in locked file cabinets
- Reception areas
- Other

Operational Safeguards

- We have:
    - a clean desk policy.
    - policies and procedures regarding information security.
    - record retention and destruction schedules: (Note that we must retain customer records according to insurers' records retention policies).
- We prohibit the removal of PERSONAL INFORMATION from our offices.
- We train staff on information security and the need to safeguard PERSONAL INFORMATION.
- We provide access to PERSONAL INFORMATION on a need-to-know basis, generally based on the roles that staff performs within the MGA
- We regularly backup our electronic records and provide for their secure storage.

Technological Safeguards

- Our systems are programmed to scan for viruses.
- We use encryption for transmission of all sensitive information by electronic means
- We have rules for the use of faxes and our fax equipment is housed in a protected location away from public view.
- We ensure the use of passwords on our systems

Assessing the Program

We assess our controls as often as necessary but in no event less often than every two years. A gap analysis is prepared, which identifies where we have found weaknesses and includes the management action plan and timetable for resolution.

Training

The OPCC urges organizations to train their front-line and management staff and keep them informed, so they can answer the following questions:

- How do I respond to public inquiries regarding our MGA's privacy policies?
- What is consent? When and how is it to be obtained?
- How do I recognize and handle requests for access to PERSONAL INFORMATION?
- To whom should I refer complaints about privacy matters?
- What are the ongoing activities and new initiatives relating to the protection of PERSONAL INFORMATION at our MGA?

We provide annual training to our staff on privacy issues. Additionally, our insurance company suppliers regularly provide training sessions to our staff and Agents.

APPENDIX B

Receiving and processing access requests - the Rules

Because we obtain customer information by providing services in connection with those applications and any policies, or when monitoring Agents, any activity we undertake relating to customers' Personal Information obtained for these purposes must be accomplished through or on behalf of the insurance company. Customer information is generally covered by their consent when processing applications for submission. We may access other customer information that Agents house on our systems or provide to us in order to assist the Agent in a sales function, for example.

When we receive an access request from a customer, we must determine whether the information requested was collected on behalf of the insurer or Agent. For example, when an Agent performs a needs analysis with a customer, he or she collects quite a bit of information that is not provided to the insurer that is ultimately asked to provide insurance. We may provide software support to the Agent to house his or her client files, including needs analyses. In addition, we may access these client files from time to time in order to fulfill our monitoring obligation delegated by the insurers or to support an Agent in the sale. If a customer wishes to access the needs analysis only, the Agent will have to respond to the request. Realistically, any access request will be more general and will involve information collected on behalf of both insurer and Agent. In contacting both Agent and insurer, from time to time we may be asked to respond on their behalf. If we do so, we require written instructions from both parties.

Should an individual wish to access their personal information, the request must be made in writing to Experior's compliance officer, Connor Moseley, at compliance@experiorheadoffice.ca, or:

Experior Head Office
660 Speedvale Ave. W, Suite 205
Guelph, ON
N1K 1E5

The following rules apply:

- The response to a customer's access request must be made within 30 days. This can be extended for a maximum of 30 additional days, if:

- Responding to the request within the original 30 days would unreasonably interfere with the parties' activities

- More time is necessary to conduct consultations or to convert PERSONAL INFORMATION to an alternate format.

- If a time extension is needed, the individual must be notified within 30 days of receiving the request, and of his or her right to complain to the OPCC.

- Assistance must be provided to any customer who needs to prepare a PERSONAL INFORMATION request.

- The individual may be asked to supply enough information to enable the parties to account for the existence, use and disclosure of PERSONAL INFORMATION.
- Access must be provided at minimal or no cost to the individual.
- The individual must be notified of the approximate costs before processing the request and asked to confirm that the individual still wants to proceed with the request.
- The requested information must be understandable, and acronyms, abbreviations and codes must be explained.
- The parties must send any information that has been amended, where appropriate, to any 3rd parties that have access to the information. This includes MGAs.
- The individual must be informed in writing when an access request is refused, setting out the reasons and any recourse available.

Customer Access Requests - Our Procedures - If we receive a request directly from a customer or through an Agent on a customer's behalf:

- Ask the requestor to name the insurer(s) involved. Do not disclose any information to the requestor. We have no regular contact with customers and cannot set up an authentication process that is robust enough to allow us to release PERSONAL INFORMATION. Even confirming the existence of insurance policies is inappropriate because we have not authenticated the requestor and ensured that he or she is entitled to the information.
- Do not attempt to discuss any concerns that might have given rise to the request. Remember that well-meaning conversation with customers can often help them "crystallize" a complaint when in fact their original intention was not to complain.
- If the requestor is the Agent, ensure that the Agent understands the process to be followed and that any customer PERSONAL INFORMATION collected on behalf of the insurer is not released directly to the Agent.
- Anyone, including the Agent, making a request on someone else's behalf needs written authorization from the owner of the PERSONAL INFORMATION. Make sure the requestor knows this.
- Notify the PC Officer of the request.
- The PC Officer should notify the Agent and/or insurer(s)' contact person directly and ask for written instructions as to whether they will handle the request or require us to be involved. We will require instructions on handling any PERSONAL INFORMATION in our possession, including whether the information needs to be provided in a certain format, the deadlines for providing the information, etc.
- **Agent or Employee Access Requests:** Notify the PC Officer, who will handle all such requests or delegate as needed.

APPENDIX C

Receiving and Responding to Inquiries and Customer Complaints – Our procedures

If we receive a privacy-related complaint directly from a customer or through an Agent on a customer's behalf:

- Do not volunteer information about policies or insurers involved. Explain that the complaint will have to be made directly to the Agent and/or insurer(s) involved. Ask the requestor to name the insurer(s).

- Do not engage in discussions with the complainant about the complaint. Once again, you don't want to be in the position of helping individuals "crystallize" their complaints.

- Notify the PC Officer. The PC Officer should:

- notify the insurer(s)/Agent involved and ask for written instructions if our assistance is required in providing PERSONAL INFORMATION or resolving the complaint;

- ask the parties to keep us apprised so that we can record the decision and make any necessary changes to our policies and procedures and close the complaint off in our complaint log.

- **Agent or employee inquiries or complaints:** Notify the PC Officer, who will handle all such inquiries or complaints, or delegate as needed.