WEALTHBRIDGE

Privacy Policy

WEALTHBRIDGE GROUP LTD.
Date: August 30, 2013

PURPOSE

Organizations in Canada are obligated to comply with the Personal Information Protection and Electronic Documents Act ("PIPEDA"). PIPEDA was created to set out ground rules for the management of personal information in the private sector and is designed to balance an individual's right to the privacy of personal information with the need of organizations to collect, use or disclose personal information for legitimate business purposes.

This Privacy Policy shall apply to WealthBridge Group Ltd. ("WBG"), as well as its related entities, WealthBridge Investment Counsel Inc. ("WBIC") and WealthBridge Financial Services Inc. ("WBFS"). Throughout this document, any reference to WBG will include WBIC and WBFS. All employees of these entities shall be bound by the policies herein, and shall not collect, use or disclose personal information except as set out in this Privacy Policy.

PERSONAL INFORMATION

PIPEDA defines personal information as any factual or subjective information about an identifiable individual that includes any personal information (recorded or not) in any form including digital or paper format. Items that would be considered personal information include (but are not limited to): name, address, phone number, gender, any identification numbers, income or other financial data. For employees it includes such items as evaluations, opinions, and disciplinary actions, as well as any other information found in an employee file (excluding the employee's name, business title, business address, and business phone number).

OBLIGATIONS

The PIPEDA establishes a set of ten principles of fair information practices that organizations must follow when collecting, using and disclosing personal information in the course of commercial activities. These principles give individuals control over how their personal information is handled in the private sector. An organization is responsible for the protection of personal information and the fair handling of it at all times, throughout the organization and in dealings with third parties. Care in collecting, using and disclosing personal information is essential to continued consumer confidence and goodwill.

The ten principles of fair information practices are:

1) ACCOUNTABILITY

The PIPEDA states that an organization is responsible for personal information under its control and shall designate an individual who is accountable for the organization's compliance with all principles of fair information practices.

To that end, WBG has appointed a Chief Privacy Officer ("CPO") who will be responsible for compliance and who shall develop and implement personal information policies and practices.

WBG's CPO will be John W. Davis, who is an owner and director of WBG, which owns 100% of the common shares of both WBIC and WBFS. Thus, the CPO will have the full support of senior management and will have the authority to intervene on privacy matters relating to the organization's operations.

The identity and contact information of the CPO will be communicated both internally and externally. This policy, as well as the contact information for the CPO will found on the WBG website: www.wealthbridge.com

Although the CPO will be responsible for policies and procedures pertaining to privacy matters, all employees of WBG and its' affiliates will be responsible for the personal information under his/her control. The CPO will ensure that all new employees of WBG and/or its' affiliates will be provided with a copy of WBG's most recent Privacy Policy, and will inform the employee that they will be obligated to abide by its' contents and acknowledge such.

The CPO will also analyze all personal information handling practices including ongoing activities and new initiatives, using the following checklist to ensure that they meet fair information practices:

- What personal information is collected?
- How and why is it collected?
- What is it used for?
- Where is it kept and how is it secured?
- Who uses it and who has access to it?
- To whom is it disclosed?
- When is it disposed of?

The CPO will also develop and implement policies and procedures to protect personal information by defining the purpose of its collection, obtaining consent (when applicable), limiting its collection/use/disclosure, ensuring that the information is correct, complete and current, ensuring that adequate security measures are in place, developing/updating a retention and destruction timetable, processing access requests, and responding to inquiries and complaints.

WBG is also responsible for any personal information under its control, including personal information that WBG may transfer to a third party for processing. WBG will take steps to ensure that the same level of privacy protection is provided by the third party when the information is being processed on WBG's behalf.

2) PURPOSE IDENTIFICATION

WBG is required to collect personal information from an individual in order to satisfy regulatory and/or legal requirements, but also to be able to provide a variety of services in a competent and professional manner. This includes (but is not limited to) such things as account opening documentation, Know Your Client Surveys, preparation of Investment Policy Statements, collection of financial data (for tax planning and preparation, financial planning and estate matters), and communications with the individuals.

In any instance, WBG will clearly identify the reasons to the individual for collecting the personal information before or at the time of collection. This identification will include an explanation as to why the information is needed, and how it will be used. This notification can be done in writing or orally.

It will be the policy of WBG that written notification will be **required** only in cases where the information that has been collected is used for a purpose other than what would ordinarily or reasonably be expected, or for a purpose not previously identified. In these cases, WBG will inform the individual of this new use, in writing (e-mail is acceptable), prior to its use and/or disclosure. This written notification will be documented and stored.

3) OBTAIN CONSENT

WBG will inform the individual in a clear and understandable manner the purposes for the collection, use, or disclosure of personal data. WBG will also obtain the individual's consent before or at the time of collection, as well as when a new use (or previously undisclosed use) is identified.

Whenever possible, express consent will be attained via signature or in writing from the individual. WBG will ensure that consent clauses are easy to find, use clear and straightforward language, not use generalized categories for purposes, uses or disclosures, and be as specific as possible as to which organizations will use the information. However, in some cases, other forms of communication may be accepted, such as verbal (in person or by phone), via email, or a note to file.

For individuals who are minors, seriously ill, or mentally incapacitated, consent may be obtained from a legal guardian, or person having power of attorney.

In cases where the personal information is considered to be of a sensitive nature, only express consent will be attained by WBG.

WBG will make it clear to all individuals that providing personal information is their personal choice and that in no way will consent be a condition for WBG to supply a product or service (unless the information is required for regulatory or legal purposes). Furthermore, WBG will make it clear to individuals that they can withdraw their consent at any time, and will explain the implications of doing so.

4) LIMIT COLLECTION

WBG will only collect personal information that it requires, either to satisfy regulatory or legal requirements, and/or to provide services in a professional manner. Thus, WBG will not collect personal information indiscriminately, nor will WBG deceive or mislead individuals about the reasons for collecting the personal information.

5) LIMIT USE, DISCLOSURE AND RETENTION

WBG will ensure that it will use or disclose personal information only for the purpose for which it was collected. Any deviation from its original purpose will require consent from the individual prior to, or at the time the information is used or disclosed.

WBG will retain personal information only as long as necessary to satisfy the purpose, or as mandated by regulatory or legal bodies.

When no longer required, personal information will be destroyed or erased in a manner that prevents improper access. In all cases, paper files will be shredded and disposed of confidentially. Electronic files will be permanently erased.

The CPO will conduct regular reviews to assess whether information is still required.

6) ACCURACY

WBG will take reasonable steps to ensure that the personal information that is used to make decisions about the individual is correct and timely. WBG will rely on the information provided by the individual, but will stress the importance to the individual that he/she provide complete and accurate information, and that WBG be kept informed of any material changes in a timely fashion (this is found in the Management Agreement as well as on the last page of the Quarterly Reporting Package).

Personal information will only be updated when necessary to fulfil the specified purposes.

7) SAFEGUARDING & PROTECTING PERSONAL INFORMATION

WBG will take steps to protect personal information against loss or theft, as well as take appropriate measures to safeguard personal information from unauthorized access, distribution, disclosure, copying, use or modification, regardless of the format in which it is held.

These measures will be taken in a variety of methods:

- All WBG employees (as well as any contractors to WBG who come in contact with any client personal information) will be required to treat all client personal information as private and confidential and are **not** permitted to communicate, share, distribute, discuss, copy, or use this information in any way, other than as required to provide the service(s) to the client as per the client's intentions. Any deviation from this by the employee could result in disciplinary action (including dismissal) if so deemed by the CPO and/or the Managing Directors;

- The WBG office will be highly secure, with access provided only to WBG personnel via secured card keys. Non WBG personnel can only enter the office upon notification and they must be permitted to enter by a WBG employee;

- Employee work stations, as well as all personal information storage, will be limited to the upper floor of the WBG office. Clients and other non WBG personnel will only have access to the lower floor where no personal information will be kept. Non WBG individuals will only gain access to the upper floor

provided they are accompanied by a WBG employee, which should only occur in rare circumstances;

- It is the policy of WBG that all personal information for an individual is on a need to know basis only. That is, personal information should only be used or accessed in the course of providing that individual with the service they require;
- All personal information that is in paper form will be kept under lock and key, either in employee work stations, or in locked filing cabinets. Access will only be provided to those employees who require access to those records in order to perform their duties;
- Employee will ensure that work stations are kept clear of any personal client information during non-office hours (in a secure and locked compartment) as well as when the employee is not working on those documents during working hours;
- All personal information that is kept in electronic form will be protected by password, and access will only be provided to those employees who require access to those records in order to perform their duties;
- All vital personal information, that is in paper/document form, that may have any perceived market value will be kept in a fireproof container at the WBG office;
- Appropriate technological safeguards will also be maintained, including encryption as well as the use of firewalls;
- Personal digital assistant devices (such as smartphones) will require password protection that is known only by the relevant employee;
- Workstation screen savers will become locked and password protected after 15 minutes of inactivity. Employees will be required to lock their computers when they plan to be away from their workstations;
- Client access to portfolio valuation statements, via the internet (through our website), is provided and is protected using a variety of naming and password conventions;
- Departing employees will be required to return keys, fobs and any other company provided access equipment. WealthBridge will take immediate steps to change any common passwords that the departing employee may have had access to;
- In cases where WBG provides personal information to a third party (after receiving consent from the individual to do so), WBG will require that the third party abide by WBG's privacy policy as a minimum. Also WBG will ensure that only the information that the third party requires to provide the service is given;
- In cases were a regulatory body requires access to personal information, WBG will be obligated to provide access to such information. In all cases, WBG will ensure that only the information they require will be provided.

8) OPENNESS

WBG's Privacy Policy has been written in a clear and concise manner to foster an environment of openness and to ensure that the policy is easily understandable. Clients and employees will be informed that WBG has established policies and practices for the management of personal information. All new employees will be given a copy of WBG's Privacy Policy, and all clients will have access to this Policy document via the web, or by paper copy upon request.

Clients will be made aware of the name, title and address of the person accountable within the organization for our privacy policies and practices. They will also be made aware of how they can gain access to their personal information, and to whom they can complain should a privacy concern arise.

9) ACCESS TO PERSONAL INFORMATION

An individual who wishes to review or verify the personal information held by WBG, or to find out to whom the information has been disclosed, may make the request for access, in writing, to WBG's Chief Privacy Officer. Upon verification of the individual's identity, the CPO will respond within 30 days (with the ability to extend for another 30 days as per subsection 8(4) of the PIPEDA).

WBG will assist the individual in any manner required to gain access to their personal information, and will do so at no cost to the individual. WBG will provide an explanation as to how the information was collected, how it is being used, and to whom it was disclosed (except where WBG is not allowed to provide such information due to regulatory or legal restrictions). In the case where WBG denies access, it will do so in writing, setting out the reasons as well as any recourse available to the individual via the Privacy Commissioner of Canada.

Upon notification from the individual of any errors or inaccuracies in the personal information, WBG will make the appropriate changes as soon as possible, provided the individual can substantiate them.

A record of all requests for information will be maintained and stored, as well as the WBG response.

10) RECOURSE

Any individual who lodges a complaint regarding WBG's compliance with any element of this Privacy Policy can do so by simply filing the complaint with the Chief Privacy Officer (John W. Davis), as follows:

Chief Privacy Officer
WealthBridge Group Ltd.
Address:
200 Doll Block
116 – 8th Avenue S.E.
Calgary, Alberta T2G 0K6
Phone: (403) 263-6004
e-mail: privacy@wealthbridge.com

Upon receipt of the complaint, the CPO will immediately do the following:

- Promptly acknowledge receipt of the complaint with the individual;
- Contact the individual to clarify the nature of the complaint, if necessary;
- Record the date the complaint is received, who filed the complaint, and the nature of the complaint;
- Investigate the matter, or assign someone within the organization to investigate the matter;
- Notify the individual of the outcome of the investigation in a clear and prompt manner, informing him/her of any steps taken to resolve the matter;
- Correct any errors or inaccuracies in the personal information, provided the individual has established proper support to do so;
- Modify or change any policies and procedures based on the outcome of the complaint and ensure that every staff member is advised of any changes;
- In the event that the individual does not feel that the matter was resolved appropriately, advise them of their recourse with the Office of the Privacy Commissioner of Canada.