

## **ONBUSINESS CHARTERED ACCOUNTANTS PRIVACY POLICY**

**Onbusiness Chartered Accountants** collects uses and discloses personal information in the possession, or under the control, of its clients to the extent required to fulfill its professional responsibilities and operate its business. The firm is committed to maintaining the privacy of personal information provided by its clients and protecting all personal information in its possession or control. This Privacy Policy sets out the principles and procedures that the firm follows in meeting its privacy commitments to its clients and complying with the requirements of federal and provincial privacy legislation.

### **Principle #1:**

**The firm is accountable for personal information in its possession or control.**

The firm is accountable for all personal information in its possession or control. This includes any personal information that the firm received directly from clients who are individuals, or indirectly, through clients that are organizations (e.g., corporations, government entities, not-for-profit organizations).

The firm has:

- established and put into effect policies and procedures aimed at properly protecting personal information;
- educated its partners and employees regarding its privacy policy and their role and responsibilities in keeping personal information private; and
- appointed its Chief Privacy Officer to oversee privacy issues at the firm.

### **Principle #2**

**The firm identifies the purposes for which it collects personal information from clients before it is collected.**

The firm collects personal information from clients and uses and discloses such information, only to provide the professional services that the client has requested. Each service the firm provides is described in an engagement letter with the client. The engagement letter includes a description of the personal information the firm will require, why it is required, the uses that will be made of the information, and with whom it may be shared in the course of providing the firm's professional services

The personal information collected from a client during the course of a professional service engagement may be:

shared with the firm's personnel participating in such engagement;  
disclosed to partners and employees within the firm to the extent required to assess compliance with applicable professional standards and rules of professional conduct, and the firm's policies, including providing quality control reviews of work performed;  
Disclosed to members of the organization's audit committee and board of directors, and others in the company that might not otherwise have access to the information, in the course of communicating aspects of the results of our audit; and  
provided to external professional practice inspectors (e.g., representatives of the Canadian Public Accountability Board, or a provincial institute of chartered accountants), who by law, professional regulation, or contract have the right of access to the firm's files for inspection purposes.

### **Principle #3**

**The firm obtains a client's consent before collecting personal information from that client.**

Before the firm undertakes a professional services engagement, it requires the prospective client to sign an engagement letter or contract. The engagement letter or contract includes a description of the personal information the firm will require, why it is required, the uses that will be made of the information, and with whom it may be shared in the course of providing the firm's professional services. By signing the engagement letter or contract, the client provides its agreement that proper consents to the collection, use and disclosure of personal information as set out in the letter have been or will be obtained (the consent of the individual is the responsibility of the client not the auditor).

### **Principle #4**

**The firm collects only that personal information required to perform its professional services and operate its business, and such information is collected by fair and lawful means.**

### **Principle #5**

**The firm uses or discloses personal information only for purposes for which it has consent, or as required by law.**

The firm retains personal information only as long as necessary to fulfill those purposes.

As required by professional standards, rules of professional conduct and regulation, the firm documents the work it performs in records, commonly called working paper files. Such files may include personal information obtained from a client.

Working paper files and other files containing, for example, copies of personal tax returns are retained for the time period required by law and regulation, including Rules of Professional Conduct.

The firm regularly and systematically destroys, erases, or makes anonymous personal information no longer required to fulfill the identified collection purposes, and no longer required by laws and regulations.

### **Principle #6**

**The firm endeavors to keep accurate, complete, and up-to-date, personal information in its possession or control, to the extent required to meet the purposes for which it was collected.**

Certain customer and other information is used to form an opinion in an audit and needs to be accurate to be relied upon, as a result, updating the information is encouraged on an annual basis.

### **Principle #7**

**The firm protects the privacy of personal information in its possession or control by using security safeguards appropriate to the sensitivity of the information.**

Physical security (e.g., restricted access, locked rooms and filing cabinets) is maintained over personal information stored in hard copy form. Partners and employees are authorized to access personal information based on client assignment and quality control responsibilities.

Authentication is used to prevent unauthorized access to personal information stored electronically. Encryption is used to prevent unauthorized access to personal information received or sent over the Internet.

For files and other materials containing personal information entrusted to a third party service provider (e.g., a provider of paper based or electronic file storage), the firm obtains appropriate assurance to affirm that the level of protection of personal information by the third party is equivalent to that of the firm.

### **Principle #8**

**The firm is open about the procedures it uses to manage personal information.**

Up-to-date information on the firm's privacy policy can be obtained from the firm's Privacy Officer (see contact information under principal 1) or at the firm's web site.

### **Principle #9**

**The firm responds on a timely basis to requests from clients about their personal information which the firm possesses or controls.**

Individual clients of the firm have the right to contact the engagement partner in charge of providing service to them and obtain access to their personal information. Similarly, authorized officers or employees of organizations that are clients of the firm have the right to contact the engagement partner in charge of providing service to them and obtain access to personal information provided by that client. In certain situations, however, the firm may not be able to give clients access to all their personal information. The firm will explain the reasons why access must be denied and any recourse the client may have, except where prohibited by law.

### **Principle #10**

**Clients may challenge the firm's compliance with its Privacy Policy.**

The firm has policies and procedures to receive, investigate, and respond to clients' complaints and questions relating to privacy.

- To challenge the firm's compliance with its Privacy Policy, clients are asked to provide an email message or letter to the firm's Privacy Officer (see contact information below).

The firm's Privacy Officer will ensure that a complete investigation of a client complaint is undertaken and will report the results of this investigation to the client within 30 days.

- If you have any questions about the firm's privacy policies and practices, the firm's Privacy Officer can be reached by email at (admin@onbusiness.ca), by phone at ((204)-985-6767) and by letter (100-1602 St.Mary's Rd Winnipeg MB R2M 3W5).