**Privacy Policy**

Last updated: 21/01/2021

This page informs you of our policies regarding the collection, use and disclosure of Personal Information we receive from users of the Site.

We use your Personal Information only for providing better services to you, the end user. By using the Site, you agree to the collection and use of information in accordance with this policy.

**Introduction**

The firm, GVNKA & Associates, collects, uses and discloses personal information in the possession of, or under the control of its clients to the extent required to fulfil 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 ten 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 – ACCOUNTABILITY

The firm is accountable for all personal information in its possession or control. This includes any personal information that the firm receives 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;

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. The types of information that may be collected for this engagement, and the purposes for which it is collected, are set out under Principles 3 and 4 of this privacy statement.

* Principle #2 – IDENTIFYING PURPOSES

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.

We collect Your IP address for the purposes of system administration, including diagnosis of problems with the firm’s server and administration of the firm’s website. All information collected will be done in a fair and lawful manner. Refer “Log Data” below.

Our website does use cookies. A “cookie” is information that our website places on your hard disk so that it can remember information about you the next time you visit our website (so that we can provide you with personalized services), measure traffic patterns (so that we can learn which browsers are commonly used), and estimate audience size (so that we can know which visitors have seen particular parts of the website). You can still navigate through our website without the use of cookies, but your access and the functionality of the website may be limited.

* Principle #3 – CONSENT

The firm obtains a client’s consent before collecting personal information from that client. The Terms and Conditions of every professional services engagement are documented in each Engagement Letter. These Terms and Conditions include an explanation about how we may use and disclose your personal information. By signing the engagement letter, you will be providing your consent to the collection, use and disclosure described in the Terms and Conditions.

Such personal information could include home addresses, home telephone numbers, financial information (credit ratings, personal indebtedness), personal information (e.g., employment history, references to criminal records) etc.

Employment candidates will also be advised of the purposes for which their personal information is being collected and you will be provided an opportunity to consent to the collection, use and disclosure as described.

You always have the option not to provide your consent to the collection, use and distribution of your personal information, or to withdraw your consent at a later stage. Where a client chooses not to provide us with permission to collect, use or disclose personal information, we may not have sufficient information to provide you with our services. Where a candidate for employment chooses not to provide us with permission to collect, use or disclose personal information we may not be able to employ you.

* Principle #4 – LIMITING COLLECTION

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

The partners and staff involved in an engagement need access to some or all of the types of personal information, noted under principle 3 above, to obtain evidence to support the firm’s opinion on the company’s financial statements or to facilitate the completion of special projects as engaged by the client. Such personal information will be a significant component of various transactions and events affecting the financial statements that will be subjected to confirmation, testing, analyses and such other procedures as the firm considers necessary to perform an audit in accordance with generally accepted auditing standards or a special project.

* Principle #5 – LIMITING USE, DISCLOSURE & RETENTION

The firm uses or discloses personal information only for purposes for which it has consent, or as required by law. We may also disclose personal information without consent:

* to comply with a warrant or an order made by a court or other body with appropriate jurisdiction or to comply with rules of conduct required by regulatory bodies.
* to a government institution that has requested the information, identified its lawful authority, and indicates that disclosure is for the purpose of enforcing, carrying out an investigation, or gathering intelligence relating to any federal, provincial or foreign law; or suspects that the information relates to national security or the conduct of international affairs; or is for the purpose of administering any federal or provincial law.
* to an investigative body or government institution on our initiative when we believe the information concerns a breach of an agreement, or a contravention of a federal, provincial, or foreign law, or we suspect the information relates to national security or the conduct of international affairs.

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 papers are safeguarded against inappropriate access, as discussed under Principle “7”.

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 or for the time period as specified in the firm’s retention of client information policy.

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.

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 team members 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;
* Principle #6 – ACCURACY

The firm endeavours 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.
Individual clients are encouraged to contact the firm’s engagement partner in charge of providing service to them to update their personal information.

* Principle #7 – SAFEGUARDS

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 – OPENNESS

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

* Principle #9 – INDIVIDUAL ACCESS

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 – CHALLENGING COMPLIANCE

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. We ensure that a complete investigation of a client complaint will be undertaken and the results of this investigation shall be reported to the client, in most cases, within 30 days.

**Log Data**

Like many site operators, we collect information that your browser sends whenever you visit our Site ("Log Data").

This Log Data may include information such as your computer's Internet Protocol ("IP") address, browser type, browser version, the pages of our Site that you visit, the time and date of your visit, the time spent on those pages and other statistics.

**Security**

The security of your Personal Information is important to us, but remember that no method of transmission over the Internet, or method of electronic storage, is 100% secure. While we strive to use commercially acceptable means to protect your Personal Information, we cannot guarantee its absolute security.

**Changes To This Privacy Policy**

This Privacy Policy is effective as of 21/01/2021 and will remain in effect except with respect to any changes in its provisions in the future, which will be in effect immediately after being posted on this page.

We reserve the right to update or change our Privacy Policy at any time and you should check this Privacy Policy periodically. Your continued use of the Service after we post any modifications to the Privacy Policy on this page will constitute your acknowledgment of the modifications and your consent to abide and be bound by the modified Privacy Policy.

If we make any material changes to this Privacy Policy, we will notify you either through the email address you have provided us, or by placing a prominent notice on our website.

**Contact Us**

If you have any questions about this Privacy Policy, please contact us.