

Preface

CTL is committed to keeping the personal information of its customers accurate, confidential, secure and private. Our Privacy Policy has been designed to inform employees, customers, and third parties of CTL of our commitment and recognition to our obligation to meet the spirit and terms of the federal **Personal Information Protection and Electronic Documents Act (PIPEDA)**.

Our Privacy Policy incorporates and expands on the 10 principles for the protection of personal information, as devised by the Canadian Standards Association (CSA). The Privacy Policy applies to personal information about the customers of CTL and other individuals that is collected, used or disclosed by CTL.

Personal Information Protection Principles

1. Accountability

CTL is accountable for the protection of all personal information within the organization's possession or control, including any personal information that has been transferred to a third party for regulatory, legal or processing purposes.

2. Identifying Purposes

Personal information is collected to assist in the recovery of past due accounts, allowing CTL to better understand the individual's financial situation. Personal information that CTL collects from customers includes:

- the customer's name and address and other contact information, such as telephone numbers, email address;
- information about a customer's transactions with us, such as account numbers, account balances, payment history;
- credit and reference information, such as date of birth, employment information,
- driver's license, previous addresses, and general financial information;
- bank information for pre-authorized payments.

3. Consent

The knowledge and consent of an individual are generally required for the collection, use or disclosure of personal information and CTL will seek to obtain consent before or when it collects, uses or discloses personal information about an individual.

4. Limiting Collection

CTL limits the amount and type of personal information it collects to that which is necessary for the business of the utility and as permitted by law.

5. Limiting Use, Disclosure and Retention

CTL will only use the personal information for the purpose for which it was collected as identified in principle #2, unless consent is given by the individual to use or disclose it for another purpose or as is required by law. Personal information will be retained for a period of 10 years.

6. Accuracy

CTL shall take all reasonable steps to ensure that all personal information will be kept accurate, complete and up to date. Individuals may challenge the accuracy and completeness of personal information about them and have it amended, as appropriate.

7. Safeguards

In executing its responsibilities with respect to the confidentiality of personal information, CTL will employ several safeguards, appropriate to the sensitivity of the information, to protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification. Such safeguards will include physical measures, organizational measures and technological measures, for example locked filing cabinets, restricted access to offices, security clearances, limiting access on a “need to know” basis and the use of passwords and encryption.

8. Openness

CTL will make its policies and practices relating to the protection of personal information available to its customers.

9. Individual Access

Any customer of CTL can have access to the personal information about them that CTL has in its possession or control. Any customer may request that their personal information be amended for purposes of accuracy and completeness.

10. Challenging Compliance

Any customer of CTL may challenge CTL’s compliance with this Privacy Policy by contacting CTL directly.

Information Protection Policy

Information can be sensitive by its nature, and can also be sensitive due to regulations and industry standards. The types of sensitive information can include:

- Client Customer information (both for customer companies and for people as individuals)
- Financial information, including credit cards, salaries, banking, transactions and more
- Company patents, business plans, and other intellectual property
- Company business records and planning materials, including our customer list, marketing and sales efforts, product line plans, and more.
- Copyrighted materials, both which our company creates and those which we obtain under license from others

This information may reside on our computing systems or backup devices, may traverse the networks, be on paper, or be in people’s minds. All locations must be properly controlled. The rules by which information is handled are determined by the regulations, business requirements, and company commitments relating to that type of information. Put together, these are called the significance of the information.

Every employee, vendor, contractor, supplier or vendor, agent or representative of our company must be aware of the significance of the information being handled, and ensure that proper controls are applied to prevent copying, disclosure, or other misuse of the information. This Information Protection policy is a part of the overall security and privacy effort of our company. Other policies and controls may also apply, as issued by the Human Resources and Policy Committee. These are available to all employees, or on the company’s intranet site.

Penalties for violating these policies may include disciplinary actions up to termination of employment, or termination of the business relationship with our company.

Our company relies upon employees and business partners to properly develop, maintain, and operate our systems, networks, and processes which keep our sensitive information safe and properly used. This means that every person and organization handling our information has the responsibility to keep the information safe, no matter where the information is located. This includes computing systems, networks, paper copies, business processes, and verbal transmission of information

Our company's policy:

1. We will meet all applicable requirements in properly protecting the information, including:
 - (a) Laws
 - (b) Regulations
 - (c) Industry standards
 - (d) Contractual commitments
2. The protections we apply to information assets will be in proportion to the value and sensitivity of the information, and will balance the sensitivity of the information against
 - (a) The cost of controls
 - (b) The impact of the controls on the effectiveness of business operations
 - (c) The risks of disclosure, modification, destruction, or unauthorized use of the
 - (d) information
3. We will protect all types of sensitive information, including but not limited to
 - (a) Financial
 - (b) Credit
 - (c) Business transaction and planning
 - (d) Personal information, both of our employees and of our customers
4. We will ensure that these controls are accepted by all employees, vendors, service providers, representatives and associates of our company who may have access to our information. This includes ensuring that all personnel at all levels are aware of, and are held accountable for safeguarding information assets.
5. We will ensure that access to information is controlled, and based upon, job function and need-to-know criteria.
6. We will maintain proper business continuity and security procedures, including information systems, networks, resources, and business processes.
7. We will report any suspected or actual breach of these policies, and will cooperate with investigative agencies.
8. We will comply with other, related policies, including the Company's privacy policies.

Privacy for Employees

Our company values each employee, and so has a commitment to protect the personal information which we handle on behalf of the employee.

It is our policy that:

1. Our company will collect only that information about employees which is needed and relevant.

2. Our company will strive to make certain that personal information about employees is kept accurate and up-to-date.
3. Our company will use appropriate controls to ensure that this information is kept secure, and is only viewed or used by the proper personnel.
4. Information about employees will not be disclosed to any external parties unless appropriate.
5. Employees will be told how they can review information about them, make updates, and report problems.
6. Our company will comply with applicable laws, regulations, and industry standards when protecting employee information.
7. We hold our employees, vendors, contractors, suppliers, and trading partners to meet this same set of policies.

Privacy for Client Customer Data

It is a part of our company's core values that we will properly value and protect any information entrusted to us about our customers. This policy describes how we will safeguard personal and company information, to ensure peace of mind when dealing with our company.

It is our policy that:

1. Our company will collect only that information about customers which is needed and relevant.
2. Our company will not disclose information to other parties unless customers have been properly notified of such a disclosure.
3. Our company will strive to make certain that information about customers is kept accurate and up-to-date.
4. Our company will use appropriate controls to ensure that this information is kept secure, and is only viewed or used by the proper personnel.
5. Our company will comply with applicable laws, regulations, and industry standards when protecting employee information.
6. We hold our employees, vendors, contractors, suppliers, and trading partners to meet this same set of policies.

Privacy Breach Management Process

A privacy breach includes the loss of, unauthorized access to, or unauthorized collection, use, disclosure, or disposal of personal information.

If a breach occurs, CTL is required to:

- report to the Privacy Commissioner of Canada breaches of security safeguards involving personal information that pose a real risk of significant harm to individuals
- notify affected clients about those breaches, and
- notify affected individuals about those breaches, and
- keep records of all breaches.

Privacy Officer

If you have any concerns and/or questions about this policy, please contact our Privacy Officer:

Privacy Officer

CTL Law

204-9130 Leslie Street

Richmond Hill, Ontario L4B 0B9

Email: privacy@ctlaw.com

Phone: 416-781-3635

Fax: 416-781-8635

The role of the Privacy Officer at CTL is to be the primary point of contact with regards to any privacy matters as relating to CTL, its clients, employees and any other companies or individuals in the course of their business with CTL.

Key Responsibilities include but are not limited to:

- Ensuring adherence to the operational actions outlined in this policy.
- Having knowledge of the principles of PIPEDA and staying abreast of any updates to legislation.
- Involvement in policy development, implementation, and maintenance.
- Managing privacy training.
- Addressing requests regarding access and correction of protected information.
- To be informed of and keep record of any reported privacy breaches.
- Conduct periodic review of privacy practices for improvement and enhancement.
- Liaising with the **Information and Privacy Commissioner** in the event of an investigation.