CTAL Privacy Policy
personal information

Update 2023-03-27

TABLE OF CONTENTS

Since this document has not been translated by a certified translator, it is for information purposes only.

INTRODUCTION

The Coopérative de télécommunication d'Antoine-Labelle "CTAL" values privacy and the protection of personal information. To ensure the respect of information held in this regard, CTAL has adopted a Policy on the Protection of Personal Information.

The objective of this policy is to ensure responsible and transparent personal information management practices in our dealings with our customers and employees.

This policy has been drafted in accordance with the Personal Information Protection and Electronic Documents Act (S.C. 2000, c. 5). This Act describes the ways in which CTAL collects, uses, communicates, retains, or processes all personal information in the context of its activities.

Personal information is required to complete a service agreement with our customers and to recruit the personnel required for our services.

DEFINITIONS

For the purposes of this policy, the words and expressions below are used as follows:

Collect I The act of gathering, acquiring, retaining, or obtaining personal information from any source, including third parties, by any means.

Communication I The act of revealing personal information to a third party.

Consentement I Acquiescement libre à la collecte, à l'utilisation et à la communication de renseignements personnels aux fins déterminées. Le consentement peut être explicite ou implicite et peut être donné directement par la personne intéressée ou par un mandataire autorisé. Le consentement explicite peut être donné de vive voix, par des moyens électroniques ou par écrit. Toutefois, il doit toujours être non équivoque et ne pas obliger la CTAL à le déduire. Le consentement implicite désigne un consentement que l'on peut raisonnablement déduire d'un acte ou d'une omission de la part d'une personne. However, it must always be unequivocal and must not oblige CTAL to presume it. Implied consent is a consent that can reasonably be inferred from a person's act or omission.

Employee I Person paid by CTAL

Applicable Legislation or Law I Refers to all rules applicable in Quebec where CTAL's services, goods and products are offered, including federal laws, in particular legislation applicable to the protection of personal information, consumer protection, electronic commerce, information technology, as well as any other rule or standard determined by the Canadian Radio-television and Telecommunications Commission (CRTC).

Member I Person who:
- Uses, has used or requests to use CTAL products or services;
- Communicates with CTAL;
- Participates in a contest sponsored by CTAL.

Personal Information | Any information concerning a natural person that can identify him or her. Excludes general information that cannot be linked to a specific individual, such as credit information, billing records, service and equipment records, and any complaints on file.

Third party | Person (natural or legal) other than the person concerned or his or her representative who is not a CTAL member.

Use | Processing, handling and management of personal information by CTAL.

PART 1 | PRIVACY CODE

Principle 1 Responsibilities

CTAL is responsible for personal information under its control. A manager is responsible for ensuring compliance with the principles set out below. At the time of publication, this person is:

Paula Torzecka, directrice marketing, communications et service aux membres
La Coopérative de télécommunication CTAL
600, boul. Albiny-Paquette
Mont-Laurier (Québec) J9L 1L4
vieprivee@ctal.ca

1.1 CTAL is responsible for personal information in its possession or safekeeping, including information entrusted to a third party for processing. CTAL does not disclose its members' personal information to third parties, unless such third parties process the information on CTAL's account, according to CTAL's instructions and pursuant to service agreements. CTAL undertakes, by contractual means or otherwise, to provide a sufficient degree of protection for the information communicated to third parties.

1.2 CTAL has implemented policies and practices designed to ensure compliance with its privacy policy, including:

- Implementing procedures to protect personal information and ensure that CTAL complies with its privacy policy.
- Implementing procedures for handling complaints and inquiries;
- Training its employees and providing them with information about CTAL's procedures;
- Drafting explanatory documents on policies and procedures.

Principle 2 Identification of purposes

The purposes for which personal information is collected shall be identified by CTAL at or before the time the data is collected.

2.1 CTAL collects personal information for the following purposes:

- Establish, develop and maintain commercial relations with members and provide day-to-day services;
- Understand the interests, needs, expectations and preferences of its members, in order to enhance its products and services and offer new ones;
- Detect and prevent possible fraud or illegal, inadequate or inappropriate use of CTAL's products and services by ensuring that efficient, reliable and secure systems are in place;
- Supply products and services requested by the member, as well as invoicing and collecting payment for invoices;
- Establish and maintain professional relationships with employees, and ensure the integrity of these relationships;
- Respect laws and regulations.

2.2 CTAL will, by any means of communication, specify the purposes for which personal information is collected to the member before or at the time the information is collected. CTAL will provide member who requests it or will refer the member to the designated person who will be able to answer its questions.

Principle 3 Consent

Except in specific situations, members must be informed of and consent to any collection, use or disclosure of their personal information.

3.1 In certain situations, applicable legislation allows CTAL to collect, use or disclose the personal information of its members, in the absence of the member's prior consent, notably:

- If an emergency occurs that threatens a member's life, health and safety, or the lives of others;
- If personal information is required for the enforcement of a law, by order of a court or an agency with jurisdiction to compel disclosure;
- If requesting the member's consent would compromise the personal information accuracy that CTAL needs to obtain in order to prevent fraud, enforce a law or breach an agreement;
- If personal information is required to claim a debt;
- If it is in the member's interest for CTAL to obtain this personal information and the member is unable to provide consent in a timely manner.

3.2 When obtaining consent, CTAL will ensure that the member is advised of the purposes for which personal information will be used or disclosed. These purposes will be stated in such a way that the member can adequately understand them.

3.3 CTAL will generally obtain consent for the collection and disclosure of personal information at the time of collection. However, CTAL may also obtain consent after collecting personal information, but before using or disclosing it for a new purpose.

3.4 CTAL will require members to consent to the collection, use or disclosure of personal information as a condition of product or service's supply only to the extent that the collection, use or disclosure of the information is necessary to fulfill the identified purposes.

3.5 CTAL will consider the sensitivity of the personal information and the reasonable expectations of its members in selecting the appropriate consent method.

3.6 The use of products and services by a member implies consent to the collection, use and communication of personal information for the purposes identified by CTAL.

3.7 A member may revoke consent at any time, subject to legal or contractual restrictions and reasonable notice. Members may contact CTAL for further information on the repercussions of such revocation.

Principle 4 Limiting Collection

CTAL collects only the personal information that is required for the identified purposes and proceeds in a lawful and honest way.

4.1 CTAL collects personal information essentially from its members and employees.

4.2 CTAL may also collect personal information from other sources, including credit bureau, employers, or personal references, or from third parties claiming to be authorized to disclose such information, with the member's consent or as permitted by law.

Principle 5 Limiting Use, Disclosure and Retention

Personal information shall not be used or disclosed for other purposes than those for which it was collected, except with the consent of the individual or as required by law. CTAL will store personal information only as long as necessary for the fulfillment of those purposes.

5.1 In some cases, personal information may be collected, used or disclosed without the knowledge or consent of the individual concerned (point 3.1).

5.2 Unless the member or employee gives its express consent or disclosure is permitted by law or otherwise required by a court, all personal information held by CTAL, except that already available to the public, is confidential and CTAL will not disclose it to anyone other than:

- The member or employee;
- Another telecommunications company to ensure the efficient and effective provision of telecommunications services;
- A company involved in providing telecommunications or directory services to the member;
- A third party for the design, improvement, marketing a product or service's supply of CTAL;
- A mandatary whose services have been retained by CTAL to collect a member's account;
- Credit card agencies and credit bureaus;
- A third party that requests an employee's information for purposes of payroll processing, benefits and the integrity of the professional relationship;
- A third party who, in CTAL's opinion, is requesting the information as an mandatary of the member or employee;

- One or more third parties, when the member or employee consents to disclosure or when disclosure is required by law.

5.3 Only CTAL employees whose business activities or regular tasks so require have access to personal information about members.

5.4 CTAL retains personal information only as long as necessary or useful for the identified purposes or as required by law. According to the situation, where personal information has been used to decide about a member, CTAL will retain either the information itself or a statement of reasons for the decision for a sufficient period to allow the member to have access to the information or reasons.

5.5 CTAL has policies, guidelines, or measures in place for the retention and destruction of personal information of members and employees that is no longer necessary or relevant for the purposes identified in this policy or that is no longer required by law. Such personal information will be destroyed, erased, or made anonymous.

Principle 6 Accuracy of personal information

Personal information must be as accurate, complete, and up to date as is necessary for the purposes it is collected.

6.1 Personal information used by CTAL shall be as accurate, complete and up-to-date as is necessary to ensure that inappropriate information is not used for decision-making about a member or employee.

6.2 CTAL will update personal information when necessary to fulfill the purposes for which it was collected or at the member's or employee's request.

Principle 7 Safeguards

CTAL protects personal information by security safeguards appropriate to its sensitivity.

7.1 CTAL is committed to protecting personal information against loss or theft, as well as unauthorized access, disclosure, copying, use or modification. CTAL will implement physical, electronic, technological, organizational, contractual and administrative safeguards that comply with industry standards. These safeguards will be adapted depending on the support and sensitivity of the personal information. Despite our best efforts, CTAL reminds you that any disclosure of personal information entails the risk of it being intercepted by third parties whose intentions are unknown.

7.2 CTAL shall protect personal information disclosed to third parties under contractual agreements setting out the confidentiality of such information and the purposes for which it is to be used.

7.3 All CTAL employees with access to personal information are required, as a condition of employment, to respect the confidentiality of personal information.

Principle 8 Openness

CTAL must ensure that specific information about its policies and practices relating to personal information management is easily accessed by anyone.

8.1 CTAL ensures that any member or employee can obtain information about its policies and practices, including:

- To ensure that its policies and practices are easy to understand and accessible to everyone;
- Provide the position and address of the Privacy Manager, as well as the location to submit complaints and inquiries;
- Description of the type of personal information held by CTAL, including a general description of its intended use.

Principle 9 Individual Access

CTAL will inform any member and employee, upon request, of the existence of personal information concerning them, the purpose for which it is used, and whether it has been disclosed to third parties, allowing them to access this information. The member or employee may contest the accuracy and completeness of the information and, if necessary, request corrections.

9.1 Upon request, the CTAL allows the member or employee to access the personal information included in their file.

9.2 Personal information must be provided in an understandable manner, within a reasonable timeframe, and at a minimal or zero cost.

9.3 CTAL may require the member or employee to provide sufficient information to enable it to inform them about the existence, use, and disclosure of personal information. The information provided for this purpose should be used solely for that purpose.

9.4 CTAL will make necessary modifications, whether it be correction, deletion, or addition to the personal information of a member or employee, when they demonstrate that their personal information is inaccurate or incomplete. These modifications will be communicated to third parties who have access to the relevant information.

9.5 Additionally, any dispute not resolved to the satisfaction of the member or employee must be documented in their file and communicated to third parties with access to the relevant information.

9.6 In certain cases, the CTAL may be unable to provide the member or employee with the personal information it holds about them and will specify the reasons for denying access to the personal information. These reasons may include:

- The disclosure of this information would reveal confidential business information;
- The information is protected by professional confidentiality;
- The information is related to a legal situation or was obtained through an official dispute resolution process;
- The requested information was obtained during an investigation into a contractual dispute or a violation of a federal or provincial law;
- Access to the information could reveal personal details about another individual or likely jeopardize the life or safety of another person;
- The cost of providing information is excessive;
- Any other reason provided by law.

Principle 10 Complaint against non-compliance with principles

Every member should be able to file a complaint about the non-compliance with the principles outlined in the Privacy Policy by contacting in writing the person responsible for ensuring compliance within the CTAL.

10.1 CTAL has established procedures for receiving and addressing complaints and requests for information regarding its policies and practices related to the management of personal information.

10.2 CTAL will inform the member or employee who makes an information request or files a complaint to the Access and Privacy Protection Officer about the existence of relevant procedures.

10.3 Any complaint will be investigated by CTAL and, if found to be justified, CTAL will take appropriate action, including modifying its policies and practices if necessary.

10.4 Any member may file a complaint with the Office of the Privacy Commissioner of Canada or with the Access to Information Commission.

Processing personal information

This section completes the General Rules.

By becoming a member or employee of CTAL, you understand that the personal information you disclose to us enables us to provide you with the products, services, or professional relationship best suited to your needs. We only collect personal information necessary for the distribution of our products and services or in the context of the employment relationship. You have the option to choose not to provide us with your personal information. However, by making this choice, it is possible that we may not be able to provide you with the product, service, or information you have requested.

Unless you provide explicit consent or disclosure is required by judicial authorities or the law, all personal information that CTAL (including its mandataries) holds about you cannot be disclosed to anyone, except:

- Yourself;
- A person who, in the opinion of CTAL, is seeking the information as your representative;
- A company that provides you with services related to the telephone service or telephone directories, provided that the information is required for this purpose, that the disclosure is done confidentially, and that the information is only used for that purpose.

CTAL uses your personal information for some purposes, such as:
For members

- Approve your application for membership in our services;
- Maintain communication with you;
- Keep you informed of current offers and promotions on our products and services, unless you object;
- Detect and prevent potential fraud or the illegal, improper, or inappropriate use of our products and services;
- Evaluate your satisfaction with our products and services;
- Comply with laws, etc.

For employees

- Payroll processing;
- Workplace health and safety;
- Maintain the professional relationship with you;
- Comply with laws, etc.

Under no circumstances do we sell information about our members or employees, nor do we transmit information about our members or employees to other organizations.

PART 2 | GOVERNANCE OF PERSONAL INFORMATION

1. Information collected, stored, shared, and destroyed for members

1.1 Collected information

At CTAL, we collect your personal information to provide you with telecommunication services. Here are the collected details :

Categories	Informations
Identification Information	▪ First and last name ▪ Email, postal address, and location where services are delivered ▪ Primary and secondary phone numbers ▪ Date of birth ▪ Gender or non-binary
Authentication Information	▪ CTAL account number
Information about your communications with us	▪ Summary of your appointments ▪ Record, history, recordings, and summary of your communications with us ▪ Written communications via email or chat ▪ Responses to surveys or consultations ▪ Video recording from security cameras at our service point
Information about your use of our websites and applications	▪ Information collected through cookies ▪ Browsing preferences (language, etc.) ▪ Navigation paths and browsing history on our website and application ▪ IP address ▪ Information related to your device, operating system, or browser
Information about your products and services	▪ Information related to invoices and non-payments ▪ Information related to balances, deposits ▪ Information related to your transactions and operations (account or contract number, date and amount of transaction or operation, description, etc.) ▪ Information about owned products (product type, acquisition date, terms, payment methods, etc.) ▪ Information about a pre-authorized debit authorization ▪ Communications regarding outages, maintenance, and modifications concerning your services
Other information to comply with legal obligations	*Employee* ▪ Social Insurance Number (SIN) ▪ Driver's license ▪ Quebec Health Insurance Card

This list may not contain all reasons for communication and is subject to change.

1.2 Stored information

We retain all information mentioned in the previous section for the purpose of identifying you, notifying you of potential changes, and transmitting important information.

The information is stored on:

Methods used	Forms
Paper	▪ Original ▪ Copies
Digital media	▪ Flash memory card ▪ USB flash drive ▪ Computer hard drive, etc.
Cloud media	▪ CTAL server ▪ Servers of CTAL's providers ▪ OneDrive, etc.
Hard disk drive equipment	▪ Computers ▪ Servers

1.3 Shared information

The collected information may be disclosed to:

- The member itself;
- Une autre compagnie de télécommunications, pour assurer l'efficience et l'efficacité des services de télécommunications;
- Une entreprise qui participe aux services de télécommunications ou de services d'annuaires au membre;
- A financial institution to set up pre-authorized payment;
- A third party for the design, improvement, marketing, or provision of a CTAL's product or service;
- A mandatary contracted by CTAL to collect a member's account;
- Credit card issuers and credit bureaus;
- Anyone who CTAL believes is requesting the information as the member's agent;
- One or more third parties, when the Member agrees to disclosure or when disclosure is required by law.

1.4 Destroyed information

We retain personal information for a period reasonably necessary or relevant for the established purposes or as required by law. We may keep certain personal information for an extended period, even when you are no longer our member (such as for tax and financial record-keeping, security, fraud prevention, and business asset management). When personal information is no longer reasonably necessary or relevant for the established purposes, or its retention is no longer required by law, it is destroyed, deleted, or anonymized.

Once the retention period has expired, we ensure to destroy or anonymize your personal information. While destruction is a definitive elimination process, anonymization means that your personal information is modified in a way that it no longer allows for your direct or indirect identification, and this is done irreversibly.

Destruction and anonymization are carried out securely and safely, following the best applicable practices.

2. Data Retention Process

We collect personal information during phone calls, email exchanges, and on social media, as well as during in-person visits to CTAL's store, for purposes described in section 1.1 of this section.

Phone calls are recorded and stored in a secure file on CTAL's server. Only authorized employees have access to this file.

Emails are saved in the Outlook folder. Conversations on social media are retained on platforms like Meta. The CTAL account is secured with access codes, and only authorized employees have access.

The information collected (refer to section 1.1 of this section) is recorded in record-opening software for subscription, service provisioning, billing, and others. This information is stored on cloud media as described in section 1.2 of this section. Access to these software programs is restricted to authorized employees, and different levels of clearance are granted to each based on the task to be completed.

As new information is communicated to us, we update existing records.

3. Data Destruction Process

When the retention period is over, we destroy the data.

Support	Destruction methods
Paper	Shredder, preferably cross-cutting *If the documents are highly confidential: shredding and incineration*
Digital media that we intend to reuse or recycle	Formatting, rewriting, digital shredding
Hard disk drive equipment	Overwriting of data on the hard disk, or hard disk removed and destroyed when machines are replaced.
Cloud media	Data erasure and dataset purging.

4. Privacy Incident

A privacy incident can be described as the unauthorized disclosure loss of personal information or unauthorized access to such information, resulting from a breach of an organization's security measures or the absence of these measures. Additionally, we can define a privacy incident as follows:

- Unauthorized access by law to personal information;
- Unauthorized use by law of personal information;
- Unauthorized disclosure by law of personal information;
- Loss of personal information or any other breach of the protection of such information

4.1 Privacy incident handling procedure

- Reason to believe that a privacy incident has occurred;
- Mitigate the risks of harm occurring or recurring (immediate mitigation measures);
- Establish the circumstances of the incident, identify the personal information, individuals affected, and the issue;
- Determine with the designated Privacy Manager the nature of the harm. Considering but not limited to:
  - Sensitivity of the information;
  - Anticipated consequences;
  - Likelihood of use for harmful purposes

  If there is no risk of serious harm:
  - Implement other mitigation measures to reduce harm and prevent the incident from recurring;
  - Record the privacy incident in the register;
  - Continuously review the process;
- If there is a risk of serious harm, notification must be provided to:
  - The Commission d'accès à l'information du Québec - mandatory;
  - Affected individuals - mandatory, unless the notice is likely to impede an investigation by a person or body authorized by law to prevent, detect, or suppress crime or offenses;
  - Person or organization able to reduce harm - discretion (disclosure of necessary information). Privacy manager records disclosure;
  - Other mitigation measures to reduce harm and prevent recurrence;
  - Register privacy incident;
  - Review the process continuously.

4.2 Notification of privacy incidents

- CTAL's Privacy Manager;
- Commission d'accès à l'information (CAi)
- Persons concerned, except if the notice is likely to hinder an investigation by a person or organization that, under the law, is in charge of preventing, detecting or repressing crime or breaches of the law.

4.3 Deadlines for privacy incident notification

Any breach of personal information will be reported to the CTAL manager. Notification of a privacy incident is made promptly and as soon as possible after becoming aware of it.

PART 3 | PRIVACY INCIDENT REGISTER AND NOTIFICATION PROCESS

Keeping a privacy incident register is mandatory to document all events affecting or potentially affecting the confidentiality and security of personal information held by CTAL. As an essential tracking tool, this register is detailed as much as possible: it must include a description of the facts related to each incident, the causes and consequences of breaches, and the corrective measures taken to remedy them so that they do not recur. This documentation work is crucial: it allows a supervisory authority, such as the Commission d'accès à l'information (CAi), to verify CTAL's compliance with the law."

When a privacy breach occurs, the CTAL team promptly notifies the Privacy Manager and implements the following:

- Validate and classify types of personal information affected. Ensure an exhaustive list of our database, file servers and documents including personal information;
- Ensure that a thorough and impartial investigation (including digital forensics, if required) is initiated, conducted, documented and concluded;
- Identify vulnerabilities and implement solutions to address them, and perform tests to ensure that corrective measures are effective;
- Report the findings to the senior management;
- Coordinate with relevant authorities as needed;
- Coordinate internal and external communications;
- Ensure that affected individuals are properly informed, if necessary.

The intervention team meets for every actual or suspected personal information breach. If the privacy incident in question involves a breach of personal information, the intervention team must be led by the team leader.

Where the privacy incident (actual or suspected) affects personal information processed on behalf of a third-party processor (a data controller), CTAL's Privacy Manager must, as the processor, report the incident to the data controller without undue delay.

The data privacy manager will send a notification to the third party data controller which must include the following:

- "A description of the nature of the breach;
- Categories of affected personal information;
- Approximate number of individuals affected;
- Name and contact information of the team leader/person in charge of data protection for data breach response;
- Consequences of the breach of personal information;
- Measures taken to remedy the breach of personal information;
- Any information related to the privacy incident.

When the privacy incident (actual or suspected) affects personal information processed by CTAL, and CTAL acts as data controller, the following actions must be taken by the Privacy Manager:

- CTAL must determine whether the privacy incident should be reported to the appropriate supervisory authority;
- To assess the risk to the rights and freedoms of the data subject, the person responsible for the protection of personal information must conduct a risk assessment of serious harm that may affect the individuals affected by the privacy incident;
- If the privacy incident is not likely to result in a risk of serious harm to the individuals affected, no notification is required. However, the privacy incident is documented and recorded in the CTAL's incident register;
- The appropriate supervisory authority must be notified without undue delay if the privacy incident is likely to cause serious harm to the individuals affected by the incident. Any possible reason for delay must be communicated to the appropriate supervisory authority.

The privacy incident register collects the following information:

- Date or period of incident knowledge;
- Date or period when the incident occurred;
- Description of the personal information that was compromised or the reason for this lack of awareness;
- Description of the facts related to the incident;
- Number of individuals affected by the incident or an approximation, if applicable;
- A description of the reasons that lead the entity to believe that the privacy incident could pose a risk of serious harm;
- If the privacy incident poses a risk of serious harm, the dates of notifications sent to the CAi and to individuals whose personal information has been compromised, and the mention of the obligation to provide public notice;
- A description of the measures taken after the privacy incident to reduce the risk of harm.

PART 4 | COMPLAINT

If a member or employee judges that CTAL has not respected the principles set out in its policies, a written complaint may be submitted to CTAL's Privacy Manager:

Paula Torzecka, Marketing, Communication and Member Service Director
La Coopérative de télécommunication CTAL
600, boul. Albiny-Paquette
Mont-Laurier (Québec) J9L 1L4
vieprivee@ctal.ca

CTAL will investigate all complaints regarding compliance with its policies and will take appropriate measures, including necessary modifications to policies or practices. In all cases, the individual who submitted a complaint will be informed of the outcome of the investigation into the complaint.

If you are dissatisfied with the CTAL's decision following a complaint, you can contact the Commission d'accès à l'information by calling 1 888-528-7741 or by email at cai.communications@cai.gouv.qc.ca

APPENDIX 1 | CONFIDENTIALITY AGREEMENT FORM

I, undersigned, am employed by the Cooperative de Télécommunication d'Antoine-Labelle in the capacity of:

_____
Position or occupation

I declare that I have read the Privacy Policy and am aware of the current guidelines and procedures for implementation.

In the course of my duties, I act as a representative of the organization for the implementation of the Privacy Policy, and I uphold the confidentiality of personal information to which I have access in accordance with this policy and the current guidelines and procedures for implementation.

I understand that a breach of this commitment may result in disciplinary sanctions, including termination, and may expose me to civil and criminal remedies.

At the end of my employment, I will uphold this confidentiality commitment.

Date: _____

_____ _____
Printed name Signature

APPENDIX 2 | PERSONAL INFORMATION ACCESS AND RECTIFICATION FORM

Request submitted to the Coopérative de télécommunication d'Antoine-Labelle.

I, undersigned, wish to consult the following documents concerning me for the period between

_____ and _____

_____

_____

_____

_____

☐ I wish to receive a copy of these documents and I agree that transcription, reproduction, or transmission fees may be charged to me.

☐ I wish to make the following corrections and/or deletions to the personal information that is inaccurate, outdated, irrelevant, incomplete, ambiguous, or collected in violation of the law concerning me (if necessary, attach all relevant documents):

_____

_____

_____

_____

_____

Comments:

_____

_____

_____

Date: _____

_____ _____

Printed name Signature