Cooptel

télécommunications
et divertissement

PRIVACY POLICY

SEPTEMBER 2023

Prepared by Edward Smith, Legal Counsel

With the collaboration of Daniel Cooper, Legal Counsel

Reviewed by Angélique Guillot, Assistant to the Directors

Revised by Cooptel on September 5, 2024

We thank the "Fédération québécoise des coopératives de santé » (FQCS) for their collaboration.

For the readers, it is important to note that the masculine form is used in this document solely for the purpose of readability.

Table of Contents

1. Introduction

The right to privacy is guaranteed by the Quebec Charter of Human Rights and Freedoms and the Civil Code of Quebec. Furthermore, the protection of personal information is governed by the Act respecting the protection of personal information in the private sector.

This policy establishes a procedure for managing personal information within the organization to ensure that personal information about members, users, volunteers, staff, and board members is collected, held, retained, used, and disclosed in accordance with the law.

The person responsible for the protection of personal information (hereinafter: "Policy Officer") within the organization is tasked with enforcing and ensuring compliance with this policy by the organization's representatives, whether they are current or former staff, volunteers, or board members.

In this respect, the Policy Officer disseminates this policy on the organization's website and makes it available to members, users, staff, volunteers, or board members for consultation or training. Furthermore, the Policy Officer establishes the necessary directives and procedures for the implementation of this policy.

2. Objectives

This policy aims to inform the organization's members, users, staff, volunteers, and board members about the principles it applies in the management of the personal information it holds about them.

Furthermore, it outlines the rules of conduct that the organization requires its members, users, staff, volunteers, and board members to follow when they have access to personal information held by the organization about others.

In implementing this policy, the organization adheres to the following principles:

- Your consent to the collection, use, and sharing of your personal information by Cooptel;
- Our commitment to only collect necessary personal information;
- Our responsibility to ensure the security and protection of the confidentiality of your personal information;
- Our transparency regarding our practices and obligations in this regard.

In accordance with these principles, the organization periodically reviews and merges its records, updates its forms and practices, and sets up a dedicated space for the storage and consultation of personal information. The organization may also be subject to inspections by an independent evaluator to validate the quality of its personal information protection measures.

3. Definition of personal information

Personal information refers to data concerning a physical person that can be used to identify them. This information is confidential and must be treated as such.

Within the organization, the following are considered personal information: name, first name, signature, residential address, phone numbers, email address, a person's image and voice, banking/financial information, information related to their family, friends, and other associated individuals, social insurance number, health insurance number, and driver's license number, as well as any document containing this information or any document that refers to the existence of a particular individual.

4. Collection of personal information

The organization collects personal information when it has a serious and legitimate interest in doing so. Personal information may be collected through forms on its website, via phone interviews, through paper forms, or through any interaction between individuals and the organization and/or its stakeholders.

The organization collects personal information primarily for managing the following:

a) Residential and business member profiles;

b) User profiles (applicants);

c) Profiles of staff and volunteers;

d) Incidents, including those that may have potential impacts on the civil liability of the organization or any person related to it;

e) Information requests about services.

When collecting personal information, the organization retains only what is necessary for its proper functioning. The organization is able to justify the reason for requesting each piece of personal information.

The organization collects personal information directly from the person concerned unless the individual consents to the organization obtaining this information from a third party. In such a case, the organization provides the individual with the Authorization Form for the Exchange of Personal Information with a Third Party, found in Appendix 1.

However, the organization may collect personal information from a third party without the individual's consent if, although it is in their interest, it cannot be collected from them in a timely manner. This may also be done to verify the accuracy of information obtained from the individual or if authorized by law.

Information that is already public or becomes public (such as information on websites or social media profiles) may also be collected by the organization without direct transmission. In this case, the organization commits to collecting such information reasonably and with discernment. The collection of information via cookies will be clearly explained on the organization's website, and users will have the option to refuse non-essential cookies.

When the organization collects personal information from a legal entity, it informs them of the source of the information, unless it involves an investigation file created to prevent, detect, or suppress a crime or legal violation.

Before the organization collects any personal information, it informs the individual concerned of the following:

a) The purposes for which the information is collected;

b) The means by which the information is collected;

c) Their right to withdraw consent to the communication or use of the information collected;

d) The name of the third party for whom the information is being collected;

e) The contact details of the personal information protection officer;

f) The categories of people, including third parties, who may have access to the information;

g) Where their personal information will be stored;

h) The protection measures in place;

i) Their rights of access and rectification as provided by law.

If the individual concerned refuses to provide the requested personal information or to consent to the exchange of personal information with a third party, it is up to the responsible officer to decide whether or not to proceed with the transaction with the individual concerned.

5. Protection of personal information

Physical files containing confidential information are kept locked in a filing cabinet or in a designated location by the responsible person, with secure access. Staff members are prohibited from leaving the workplace with personal information without the organization's approval. The organization's offices are also secured with an access code known only to staff (lock mechanism) as well as a chip mechanism.

Electronic files containing personal information are protected by encryption or a password. Personal information is stored digitally in a secure local network that prevents individuals from accessing the organization's files.

A VPN connection is also required to access certain information. The organization has established a firewall and antivirus software to limit the scope of malicious attacks.

he categories of individuals who have access to personal information when required in the course of their duties are as follows:

a) Members of the board of directors and senior management;

b) Staff.

The organization requires anyone holding a position in either of these categories to complete the Confidentiality and Non-Disclosure Commitment Form, found in Appendix 2. The organization also ensures that the roles and responsibilities of its staff members are outlined throughout the lifecycle of this information so that they understand how to implement the policy in their daily activities.

6. Policy officer

Ms. Marie-Eve Rocheleau is responsible for the protection of personal information within the organization in accordance with Section 3.1 of the Act on the Protection of Personal Information in the Private Sector. Ms. Rocheleau is the Executive Director of the organization. She can be reached at 450-532-2667 (toll-free 1-888-532-2667) or at prp@cooptel.coop

In addition to her other duties, the responsible person also ensures that the organization's staff understands the issues related to personal information protection. She must ensure that user files are classified, stored, and destroyed securely, and that all personal information is handled with the utmost care. She is also responsible for receiving requests and complaints regarding the personal information protection policy and coordinates with the *"Commission d'accès à l'information"* when the situation requires it.

7. Use of personal information

Personal information collected by the organization is used or disclosed only for the purposes for which it was collected unless the individual consents or the law requires otherwise. Personal information is primarily used to facilitate the provision of services to members, clients, and users. However, it may also be used for market research, distribution of newsletters (which can be unsubscribed from at any time), hiring staff, or for any reason detailed at the time of personal information collection.

Personal information will never be sold to third parties unless the organization obtains consent for that purpose.

The organization also ensures that the personal information it holds about others is up-to-date and accurate at the time it is used to make decisions regarding the individual concerned.

At any time, you have the right to withdraw your consent to the use and disclosure of your personal information. To do so, you must contact the person responsible for the protection of personal information within the organization at 450-532-2667 (toll-free 1-888-532-2667) or at prp@cooptel.coop.

8. Retention and destruction of personal information

When the purpose for which personal information was collected has been fulfilled, the organization destroys it, unless exceptional circumstances exist. In accordance with the law, personal information is retained according to the applicable framework for the retention and destruction of personal information within the organization. Personal information subject to a request for access or correction is retained until all legal remedies have been exhausted. Furthermore, the organization retains personal information for the duration required by the governmental authorities to which it is accountable.

Subject to other legal/ethical obligations regarding the retention of records that the organization and the individuals working on its behalf must comply with, the individual concerned may request that any file pertaining to them be returned and that any personal information otherwise held by the organization be destroyed. The destruction of personal information may also lead to the organization being unable to continue providing goods or services. The same applies if the individual no longer consents to this policy.

The organization does not discard any document containing personal information that could be reconstructed. In such cases, these documents are destroyed or shredded. If not, the organization resorts, as applicable, to formatting, rewriting, digital shredding, demagnetization, or overwriting of the information.

9. Right of access and transfer of personal information

Upon the verbal or written request of an individual concerned, or of someone establishing their status as a representative, successor, estate administrator, life insurance beneficiary, or holder of parental authority of the individual concerned, the organization confirms whether it holds personal information related to the individual.

Upon a written request from an individual concerned or one of the persons designated in the previous paragraph, the organization allows them, within thirty (30) days of receiving the request, to consult or transfer, as applicable, their file or that of the individual concerned, and discloses any personal information recorded therein. However, the organization may refuse to disclose personal information in the following cases:

a) It does not pertain to the interests and rights of the requester as an executor or beneficiary.

b) It would likely reveal personal information about a third party or the existence of such information, and this disclosure could seriously harm that third party unless they consent. c) It is prohibited by law, an ongoing investigation, or a court order.

In case of a refusal, the organization provides a written explanation to the individual concerned within the same thirty (30) days and informs them of their right to contest the decision before the "*Commission d'accès à l'information"*. If the organization fails to respond to a request for access within this time frame, it is deemed to have denied access, in which case the interested individual may approach the "*Commission d'accès à l'information"* to assert their rights.

Notwithstanding the above, the organization cannot refuse to disclose personal information concerning an individual if it involves an emergency that endangers the life, health, or safety of the individual concerned.

However, the organization may temporarily refuse access to personal health information it holds about the individual if it could cause serious harm to their health, provided that it offers to allow a health professional designated by the individual to receive such information and communicate it to them. This professional then determines when the consultation can take place and informs the individual concerned.

Finally, unless the request is made by the holder of parental authority, the organization refuses to disclose to an individual under the age of 14 any medical or social information concerning them, or to inform them of the existence of such information contained in a file created about them, except through their lawyer in the context of legal proceedings. Normal communications between a health and social services professional and their patient are not restricted by this provision.

When a request to consult or correct personal information is made to a representative of the organization, they invite the requester to complete the Personal Information Access or Correction Request Form, found in Appendix 3, unless the request has been made in writing. They then forward the completed form from the requester or their written request to the responsible person, who ensures it is analyzed and, as applicable, determines the access modalities, how to make the requested corrections, or provides justification for any refusal.

10. Right to data portability

Upon the written request of the individual concerned or a person designated in the first paragraph of the section "Right of Access and Transfer of Personal Information," the organization will communicate the personal information file to another company or organization designated by the individual concerned, within thirty (30) days of receiving the request using the Portability Right Form, found in Appendix 7. The computerized personal information held about this individual will be transmitted in a structured and commonly used technological format such as: CSV, XML, JSON, ODT, and ODS.

The transmission of the file containing the personal information of the individual concerned must be carried out in a secure manner, taking into account, in particular, the sensitivity of the information being transmitted.

Scope of the Right to Portability and Its Exclusions

The right to portability applies only to computerized personal information provided directly by the individual concerned.

Consequently, this right does not apply to the following personal information:

- Personal information collected or stored in paper format;
- Personal information collected from third parties (for example, if we use a third-party platform to obtain application records within our organization);
- Personal information created or inferred (for example, a user profile created from a business intelligence algorithm).

The communication of a computerized file containing personal information to the individual concerned who requests it may pose new security risks. These risks affect both the individual whose personal information is the subject of the request and the organization itself.

Before communicating a file of personal information to the individual concerned or to a third party identified by this individual, and given the security risks involved, the organization must verify the identity of the requester and ensure they are entitled to make the request through a rigorous and documented validation process. Identification documents will be required from the individual concerned, along with the duly completed and signed Portability Right Form, found in Appendix 7.

11. Request for correction of personal information

Upon the written request of the individual concerned or a person designated in the first paragraph of the section "Right of Access and Transfer of Personal Information," the organization shall rectify any inaccurate, incomplete, or ambiguous information, as applicable, in their file or the file of the individual concerned, add comments, or remove outdated information that is not justified by the purpose of the file or whose collection was not authorized by law, within thirty (30) days of receiving the request.

In the event of a refusal, the organization provides a written explanation to the individual concerned within the same thirty (30) days and informs them of their right to contest the decision before the *"Commission d'accès à l'information".* If the organization fails to respond to a request for correction within this timeframe, it is deemed to have refused to comply, in which case the interested individual may approach the *"Commission d'accès à l'information"* to assert their rights.

Upon agreeing to a request for correction, the organization provides the requester with a copy of any modified or added personal information, or, as applicable, a certificate of the removal of personal information, at no charge.

The organization promptly notifies any person who received the information within the previous six (6) months of the correction or contested correction request and, if applicable, the individual from whom it obtained the information.

It is the responsibility of individuals who have provided their personal information to inform the organization of any changes regarding that information. The organization cannot be held liable for any failure to make a correction if it should have been made.

12. Communication of personal information to a third party

At the time of collecting personal information, the organization submits the Authorization Form for the Exchange of Personal Information with a Third Party, found in Appendix 1, requesting the individual concerned to complete it if they consent to the organization communicating personal information about them to third parties. The organization will inform them of the communications that will take place following this form.

When a third party not identified in the Authorization Form for the Exchange of Personal Information with a Third Party requests the organization to provide personal information regarding a member, user, staff member, volunteer, or director of the organization, the organization requires the third party to obtain written consent from the individual concerned, which must include the following information:

a) The identification of the individual concerned;

b) A description of the personal information to be communicated;

c) The identification of the third party to whom the information may be communicated;

d) The expiration date of the authorization;

e) The signature of the individual concerned or their authorized representative.

However, the organization may communicate personal information to a third party not identified on the Authorization Form for the Exchange of Personal Information with a Third Party, found in Appendix 1, if that third party is:

a) The attorney of the individual concerned;

b) The Attorney General if the information is required for a prosecution for a violation of a law applicable in Quebec;

c) A person authorized by law to prevent, detect, or suppress crime or violations of laws, who requires it in the performance of their duties, if the information is necessary for the prosecution of a violation of a law applicable in Quebec;

d) A person to whom it is necessary to communicate the information in the context of law enforcement or a collective agreement and who requires it in the performance of their duties;

e) A public agency that, through a representative, may collect information in the exercise of its responsibilities or in the implementation of a program it manages;

f) A person or organization with the authority to compel communication and who requires it in the performance of their duties (e.g., courts);

g) A person to whom this communication must be made due to an emergency situation endangering the life, health, or safety of the individual concerned;

h) A person or organization, in accordance with articles 18.1, 18.2, 18.3 (effective September 22, 2023 for this article), and 18.4 of the Act on the Protection of Personal Information in the Private Sector;

i) A person authorized to use this information for study, research, or statistical purposes;

j) A person who, under the law, can recover debts for others and who requires it in the performance of their duties;

k) A person if the information is necessary for the purpose of recovering a debt owed to the organization.

The organization must record in the file of the individual concerned any communication made under paragraphs f) to k).

When the organization entrusts another organization with the responsibility of holding, using, or communicating personal information on its behalf, it must, before disclosing this personal information, obtain written assurance from that organization that it complies with this personal information protection policy.

When the organization communicates personal information outside of Quebec, it ensures that this information will not be used for purposes unrelated to the objective of the file nor communicated to third parties without the consent of the individual concerned, except to the third parties described in paragraphs a) to j) of this section. If the organization believes that these conditions will not be met, it must refuse the communication.

13. Fees for transcription, reproduction or transmission of personal information

The organization charges reasonable fees for the transcription, reproduction, or transmission of personal information. These fees are set by the responsible person and are subject to periodic review.

Before proceeding with the transcription, reproduction, or transmission of this information, the organization informs the requester of the approximate amount due.

14. Transmission of documents containing personal information

In the case of an email transmission, the organization's representatives indicate in the subject line the confidential nature of the transmission and include a confidentiality notice in the message, inviting the recipient to contact the sender immediately in case of erroneous receipt. The representatives of the organization include their name, as well as their work address and phone and fax numbers, in the email signature.

In the case of a mail transmission, the organization's representatives clearly indicate, on the packaging, the name and address of the person authorized to receive the documents. They include a letter with the shipment specifying the confidential nature of the information and a confidentiality notice inviting the recipient to contact the sender immediately in case of erroneous receipt.

15. Definition of a confidentiality incident

In accordance with the *Act respecting the protection of personal information in the private sector*, a confidentiality incident may take the following forms:

- Unauthorized access to personal information;
- Unauthorized use of personal information;
- Unauthorized communication of personal information;
- Loss of personal information or any other breach of the protection of such information.

16. Process in the event of a confidentiality incident

In the event of an incident involving personal information, the organization ensures compliance with the procedure outlined in the Act on the Protection of Personal Information in the Private Sector and its related regulations. When an incident poses a serious risk of harm, the *"Commission d'accès à l'information"* (CAI) and the individuals affected by the incident will be notified, as circumstances permit, as quickly as possible after the organization becomes aware of the incident. The content of these notices is specified in Appendices 4 and 5, respectively.

If third parties need to be contacted to mitigate potential damages resulting from the incident, the person responsible for the protection of personal information will ensure that only the personal information necessary for this purpose is communicated and that this communication is documented. An incident register will be updated by the person responsible for the protection of personal information. The content of this register is found in Appendix 6.

By transmitting personal information to the organization, it is understood that the individuals involved recognize that the organization employs best work practices and protective mechanisms to limit the possibility of any incident, leakage, or misuse of personal information. However, the organization cannot guarantee infallible security against all conceivable scenarios.

When an individual notices that an incident involving their personal information may have occurred within the organization, they must contact the person responsible for the protection of personal information using the contact details provided above. Complaints/reports will be addressed within a maximum of thirty (30) days after submission.

17. Non-applicability of the policy

When an individual leaves the organization’s website to visit any other website linked to it, this policy no longer applies. They should then refer to that site's policy, if applicable.

When a law, regulation, or court order requires the organization to transmit personal information, it is understood that the organization cannot guarantee the level of confidentiality and security established by the individual or government that receives the information.

In the event of a merger or other legal restructuring of the organization, it may transfer all personal information to the newly created legal entity.

18. Modification of the policy

Any modifications will be updated on the organization’s website, and the latest modified version can be found at the following location: https://www.cooptel.ca/en/governance/

19. Adoption et entry into force of this policy

This policy was adopted on:	August 31, 2023
This policy comes into effect:	September 1, 2023

Appendices

APPENDIX 1 – AUTHORIZATION FORM FOR THE EXCHANGE OF PERSONAL INFORMATION WITH A THIRD PARTY

By this document, **I authorize** _____
Name of the organization

☐ **To communicate with the following individuals and organizations:**

_____ _____

_____ _____

☐ **To collect from the following individuals and organizations:**

_____ _____

_____ _____

The following information concerning me:

_____ _____

_____ _____

_____ _____

This authorization is valid:

☐ **for a period of 3 years from the date of signing this document.**

☐ **until further notice from me.**

Date : _____

_____ _____
Name of the individual concerned in printed letters Signature of the individual concerned

Date : _____

_____ _____
Name of the authorized representative in printed letters Signature of the authorized representative

APPENDIX 2 – CONFIDENTIALITY AND NON-DISCLOSURE AGREEMENT FORM

1. PURPOSE

This agreement concerns employees not bound by professional secrecy who come into contact with personal and confidential information in the course of their duties. The objective of Cooptel is to limit the sharing of this information and to protect it.

2. PERSONAL AND CONFIDENTIAL INFORMATION

This agreement pertains to personal and confidential information contained in:

- Payroll
- Employee records
- Management of group insurance
- Management of the pension plan
- Workplace accidents
- The recruitment process (interviews, references, criminal records, etc.)
- Any other sensitive information

3. EMPLOYEE COMMITMENT

The commitment involves:

- Protecting personal or confidential information.
- Not transmitting and/or communicating this information, materials, or documents to unauthorized individuals within Cooptel or externally without prior authorization to do so.
- Not publishing such information.
- Not using or disclosing such information for purposes other than authorized official purposes.
- Accepting full responsibility for ensuring the confidentiality and safeguarding of this information in the event it is entrusted to them.
- Take all reasonable measures to prevent any unauthorized person from examining and/or copying such information.

- Safely dispose of/destroy all personal and confidential information that is no longer needed (according to established timelines), regardless of the medium on which it is found: paper, electronic, or otherwise.
- Notify your immediate supervisor as soon as you detect or suspect a leak of personal or confidential information and cooperate in managing the incident.

4. DURATION OF THE AGREEMENT

The agreement applies both during the employee's tenure and after their employment with Cooptel. Any breach of these rules constitutes grounds for immediate dismissal and/or legal action.

In the course of my employment as _____ with Cooptel, I acknowledge that I have access to personal and confidential information and I commit to respecting this agreement.

Signed in Valcourt,

_____ _____

Name of the employee Signature

_____ _____

Name of the supervisor Date

Supervisor’s Position

APPENDIX 3 – ACCESS AND CORRECTION OF PERSONAL INFORMATION FORM

To: _____
Name of the organization

I wish to consult the following document(s) concerning me for the period between_____ and _____:

_____

_____

_____

_____

☐ **I wish to receive copies of these documents, and I accept that transcription, reproduction, or transmission fees will be charged to me.**

☐ **I wish to make the following corrections and/or deletions to the inaccurate, outdated, irrelevant, incomplete, ambiguous, or unlawfully collected personal information concerning me (**please specify the information to be corrected or deleted and the reasons justifying the correction. If necessary, attach any relevant documents to support your request)**.**

_____

_____

_____

_____

Additional comments

_____

_____

Date : _____

_____ _____
Name in printed letters Signature

APPENDIX 4 – CONTENT OF THE NOTICE TO THE CAI IN THE EVENT OF A CONFIDENTIALITY INCIDENT

The notice to the CAI includes:

- The name and NEQ of the organization;
- The name of the person responsible for the protection of personal information;
- A description of the personal information involved in the incident (if this information is not known, the reason justifying the inability to provide such a description);
- A brief description of the circumstances of the incident (and, if known, its cause);
- The date or period when the incident occurred (and, if unknown, an approximation);
- The date or period during which the organization became aware of the incident;
- The number of people affected by the incident and, among them, the number of Quebec residents (or, if unknown, an approximation of these numbers);
- A description of the elements leading the organization to conclude that there is a risk of serious harm to the affected individuals;
- The measures the organization has taken or intends to take to notify the affected individuals (including the date when the individuals were notified or the proposed timeframe);
- The measures the organization has taken or intends to take following the occurrence of the incident (including the date or period when the measures were taken or the proposed timeframe);
- If applicable, a mention indicating that a person or organization located outside Quebec with similar responsibilities to the CAI has been notified of the incident.

The information provided in the notice must be updated in case of subsequent changes.

APPENDIX 5 – CONTENT OF THE NOTICE TO THE PERSONS CONCERNED IN THE EVENT OF A CONFIDENTIALITY INCIDENT

The notice to the affected individuals includes:

- A description of the personal information involved in the incident (if this information is not known, the reason justifying the inability to provide such a description);
- A brief description of the circumstances of the incident;
- The date or period when the incident occurred (and, if unknown, an approximation);
- A brief description of the measures the organization has taken or intends to take following the occurrence of the incident, in order to reduce the risk of harm;
- The measures the organization suggests the affected individual take to reduce the risk of harm or to mitigate such harm;
- The contact information for the affected individual to inquire further about the incident.

The notice can be public if:

- The act of transmitting the notice is likely to cause increased harm to the affected individual;
- The act of transmitting the notice is likely to pose excessive difficulty for the organization;
- The organization does not have the contact information for the affected individual;
- The organization does not fall under one of the three cases mentioned above but wishes to inform the affected individuals quickly while still ensuring they receive a direct notice afterward.

APPENDIX 6 – CONTENT OF THE CONFIDENTIALITY INCIDENT REGISTRY

The incident register must include:

- The incident number (for internal reference);
- A description of the personal information involved in the incident (if this information is not known, the reason justifying the inability to provide such a description);
- A brief description of the circumstances of the incident;
- The date or period when the incident occurred (and, if unknown, an approximation);
- The date or period when the organization became aware of the incident;
- The number of individuals affected by the incident (or, if unknown, an approximation of that number);
- A description of the factors that lead the organization to conclude that there is a risk of serious harm to the affected individuals;
- The dates of transmission of notices to the CAI and the affected individuals, as well as a mention indicating whether public notices have been issued by the organization and the reason for doing so, if applicable;
- A brief description of the measures taken by the organization following the incident to reduce the risk of harm.

The information contained in the register must be kept up to date and retained for a minimum period of five years after the date or period when the organization became aware of the incident.

APPENDIX 7 – DATA PORTABILITY FORM

To : _____
Name of the organization

I request that the following documents concerning me be transmitted for the period between _____ and _____:

_____

_____

_____

_____

☐ **I wish to send a copy of these documents to the following company or organization, and I accept that transcription, reproduction, or transmission fees will be charged to me.**

NAME OF THE COMPANY OR ORGANIZATION:

_____

_____

_____

_____

Additional comments

_____

_____

Date : _____

_____ _____
Name in printed letters Signature