PRIVACY PROTECTION POLICY

Le service Oxili is led by Ex aequo

Adopted on March 28, 2024

Content table

INTRODUCTION

Ex aequo, a community organization for the promotion and collective defense of rights, has a personal information confidentiality policy. Given its unique confidentiality issues, it also has a specific confidentiality policy for its Le service Oxili.

Le service Oxili respects each individual's right to privacy and protects the confidentiality of personal information collected from all its users. Such information is available only to Ex aequo employees and external professional persons performing their respective duties for Le service Oxili. All these persons must first sign the confidentiality policy.

1. DEFINITIONS

1.1 Employee
Any person who works for Le service Oxili for remuneration, including management and any unpaid persons (volunteers and interns).

1.2 User
Any individual using Le service Oxili: self-managers, close caregivers, home aides, and health network interveners.

1.3 Event
Any event in which Le service Oxili participates or organizes.

1.4 Reporting form
The form is available to all users of Le service Oxili to inform the person responsible for personal information.

1.5 Confidentiality incident
Any unauthorized access to personal information by law, its use, or its communication, as well as its loss or any other form of breach of its protection.

1.6 Publication
Any publication produced by Le service Oxili or to which Le service Oxili contributes in any form (verbal, written, audio, video, computerized, or other).

1.7 Confidentiality Incidents Register
All information recorded on declared incidents regarding the incident's circumstances, the number of individuals involved, the assessment of the risk severity, and the measures taken in response to the incident. Relevant dates are also included: incident occurrence, detection by the organization, transmission of notices (if applicable), etc.

1.8 Serious risk of harm
The person responsible for personal information analyzes the risk assessed following a confidentiality incident that could harm the individuals concerned. For any confidentiality incident, the responsible person evaluates the severity of the risk of harm to the individuals concerned by estimating "the sensitivity of the information involved," "the anticipated consequences of its use," and "the likelihood of its use for harmful purposes."

1.9 Personal information
Any information provided or communicated to Le service Oxili concerning a current or potential user that can be used to identify them: their name, phone number, address, email address, gender, sexual orientation, and any health information. This information can be provided or communicated in any form (verbal, written, audio, video, computerized, or other).

For certainty:

- Information that does not allow for the identification of an individual in the context of testimony is not confidential.
- Statistical data is not confidential information as it does not allow for individual identification.
- Photographs or recordings that do not allow for the identification of an individual are not considered confidential information regarding that individual.

1.10 Service or Activity
Any service that Le service Oxili provides to an individual upon their request or any activity they participate in.

2. PHOTOGRAPHS AND RECORDINGS

2.1 Every individual has the choice to be photographed or not or to be recorded (audio/video) or not.

2.2 Photographs or recordings that identify an individual as an employee of Ex aequo for Le service Oxili are not considered confidential information regarding that individual.

3. CONFIDENTIALITY OBLIGATION

3.1 Ex aequo employees must sign a confidentiality agreement before performing their duties or carrying out their mandates for Le service Oxili.

3.2 The confidentiality obligation applies for the duration of a person's volunteering, internship, contract with a professional, or employment relationship with Ex aequo. This obligation remains even after the end of the person's volunteering, internship, contract, or employment relationship with Ex aequo.

4. COLLECTION AND USE OF PERSONAL INFORMATION

4.1 Le service Oxili may, if necessary, create one or more files containing personal information about users. The purpose of creating such files is to:

- Maintain updated contact information;
- Document user profiles.

4.2 Le service Oxili creates files containing personal information about users. This information is used to enable Le service Oxili to provide services and sometimes carry out an activity or publication.

4.3 Le service Oxili may only collect personal information necessary for the purpose of the file and may only use personal information for those purposes.

4.4 Personal information may only be collected from the individual concerned unless they consent to the collection being carried out by their representative or if the law permits it.

5. MANAGEMENT OF PERSONAL INFORMATION

5.1 The person in the general management of Ex aequo is mandated by the board of directors to be responsible for ensuring personal information protection. It must be indicated on Ex aequo's website that the person in the general management is also the "person responsible for the protection of personal information" and how to contact them.
The responsible person ensures the maintenance of a Confidentiality Incidents Register.

5.2 Subject to Article 5.3, employees are authorized to access any personal information Le service Oxili holds. Management and an external professional are authorized to access personal information to the extent necessary to perform a task in the exercise of their functions.

5.3 For the application of laws, a confidentiality incident corresponds to any unauthorized access, use, or communication of personal information by law, as well as the loss of personal information or any other breach of its protection.

5.4 When an employee or user notices a confidentiality incident, they must promptly inform the person responsible for protecting personal information so that it is recorded in the Register. The employee or user must complete a reporting form and submit it to the person responsible for protecting personal information.

The register must retain information on a confidentiality incident for a period of five years. The reporting form must include:

- A description of the personal information affected by the incident or, if this information is unknown, the reasons why it is impossible to provide such a description;
- A brief description of the incident's circumstances;
- The date or period when the incident occurred (or an approximation if this information is unknown);
- The date or period when the organization became aware of the incident;
- The number of individuals affected by the incident (or an approximation if this information is unknown).

5.5 The responsible person determines if the incident presents a "serious risk of harm." The information and measures to be taken to reduce the risk of serious harm to the individuals concerned are recorded in the Register.
Suppose the incident presents a severe risk of harm. In that case, the responsible person notifies the Commission for Access to Information and the individuals concerned of any incident presenting a serious risk of harm using the appropriate form.

6. RETENTION OF PERSONAL INFORMATION

6.1 Employees with access to files under Article 5 are required to:

- Ensure that personal information is protected from any physical damage or unauthorized access;
- Ensure all electronic documents containing personal information, including those copied to a portable storage device, are encrypted and password-protected. Password management follows a proven method;
- Personal information must be kept in paper format in lockable filing cabinets. The cabinets must be locked at the end of each workday, and the keys must be held securely.

6.2 When an employee can also be qualified as a user, personal information regarding each title will be kept separately.

6.3 The files of users created under this policy are the property of Le service Oxili.

7. DESTRUCTION OF PERSONAL INFORMATION

7.1 Subject to Article 7.2, personal information is retained as long as the purpose for which it was collected remains unchanged unless the individual concerned has consented otherwise. This personal information is then destroyed so that the data it contains can no longer be reconstructed.

7.2 Le service Oxili retains files concerning users. Files of home aides with a "permanently inactive" status for 7 years are destroyed, while files of self-managers who become "permanently inactive" are destroyed immediately.

7.3 For certainty, confidential information about an individual who has provided testimony, such as their name and contact details, is destroyed once the testimony is published or broadcast unless the individual has previously consented to the confidential information being retained to allow Le service Oxili to recontact them in the future. For certainty, each use of an individual's testimony must be approved by that individual.

8. DISCLOSURE OF PERSONAL INFORMATION TO THIRD PARTIES

8.1 Except where required by law and subject to the other provisions of Article 8, personal information may only be disclosed to a third party after obtaining the express, free, and informed verbal or written consent of the individual concerned or their representative. Such consent can only be given for a specific purpose and for the necessary duration.

8.2 Home aides must sign a consent form to disclose personal information.

8.3 Personal information may be disclosed without the individual's consent if their life, health, or safety is seriously threatened. The disclosure must be made in the least harmful way for the individual concerned.

8.4 As permitted by law, Le service Oxili may disclose the personal information necessary for its defence or prosecution against a user or their heirs, executors, or assigns, including any claim from the user's insurer.

9. COMMUNICATION OF PERSONAL INFORMATION TO THE INDIVIDUAL CONCERNED

9.1 Subject to Article 9.2, users have the right to know the personal information that Le service Oxili has received, collected, and retained about them, to access such information, and to request corrections to it.

9.2 Le service Oxili must restrict access to personal information when required by law or when disclosure would likely reveal confidential information about a third party.

9.3 A user's request related to Article 9.1 must be processed within a maximum of 30 days.

10. BREACH OF CONFIDENTIALITY OBLIGATION

10.1 An employee breaches their confidentiality obligation when they:

- Communicate personal information to individuals not authorized to access it;
- Discuss personal information inside or outside Le service Oxili premises where unauthorized individuals might overhear it;
- Leave personal information on paper or electronic media in view in a place where unauthorized individuals might see it;
- Fail to follow the provisions of this policy.

10.2 In the event of a breach of confidentiality, appropriate disciplinary measures, up to and including termination of a service contract or any other relationship with Le service Oxili, will

be taken against the offending party, and corrective measures will be adopted as needed to prevent such a scenario from recurring.

11. REMEDIES

11.1 If it is encountered that a person's personal information has been used contrary to a provision of this policy, that person may file a complaint with the person responsible for personal information at Ex aequo or with the Ex aequo board of directors if the complaint concerns the person in general management.

11.2 As provided by law, a person denied access to or correction of their personal information may file a complaint with the Commission for Access to Information for review within 30 days of Ex aequo's refusal to comply with their request or the expiration of the response time.

ANNEX A: REPORTING FORM

As the Privacy Protection Policy provides, you must fill out this reporting form as soon as you notice a confidentiality incident and submit it to general management. The collected information will be documented in the Confidentiality Incidents Register. Based on this information, general management will decide if the incident presents a "serious risk of harm" to the individuals concerned and will file a declaration with the Access to Information Commission if necessary. Measures to control and prevent the type of incident reported will then be deployed.
A confidentiality incident corresponds to any unauthorized access, use, or communication of personal information by law, as well as the loss of personal information or any other breach of its protection.
For example, a confidentiality incident may occur when:

- A team member consults personal information without authorization;
- A team member communicates personal information to the wrong recipient;
- The organization is a cyberattack victim: phishing, ransomware, etc.

ANNEX B: CONFIDENTIALITY INCIDENT REPORT FORM (INTERNAL DOCUMENT)

Date and period of the confidentiality incident

Date of the incident:

Date of the discovery of the incident:

The incident occurred throughout:

Type of confidentiality incident (identify with an "x" the type of incident):

☐ Unauthorized access to personal information by law
☐ Unauthorized use of personal information by law
☐ Unauthorized communication of personal information by law
☐ Loss of personal information or any other breach of its protection

Causes and circumstances of the incident (identify with an "x" the causes or circumstances):

☐ Deliberate alteration
☐ Accidental communication
☐ Deliberate communication without authorization
☐ Unauthorized consultation
☐ Cyberattack (virus, spyware, etc.)
☐ Technical failure
☐ Accidental destruction
☐ Deliberate destruction without authorization
☐ Accidental disclosure
☐ Deliberate disclosure without authorization
☐ Human error
☐ Phishing
☐ Social engineering (manipulation technique to obtain personal information)
☐ Loss of access to information
☐ Loss of information
☐ Ransomware
☐ Incompatible use
☐ Information theft
☐ Other, specify:

On what medium was the personal information stored during the incident?

☐ Office computer
☐ Home computer

☐ Electronic removable device
☐ Paper
☐ USB key
☐ Server
☐ CD
☐ Sound recording
☐ Mobile phone
☐ Cloud
☐ Tablet
☐ Video surveillance
☐ Laptop
☐ Photo
☐ Other, specify:

Identification of personal information affected by the confidentiality incident (identify with an x for each piece of information):

☐ Name
☐ First name
☐ Home address
☐ Date of birth
☐ Home phone number
☐ Cell phone number
☐ Personal email address
☐ Driver's license number
☐ Social insurance number
☐ Health insurance number
☐ Passport number
☐ Salary, Position / Occupation
☐ Information about employees or beneficiaries
☐ Medical information
☐ Genetic information
☐ School / academic information
☐ Banking information/account number/institution/investments/mortgage
☐ Credit card number
☐ Personal identification number (PIN)
☐ Cardholder's name
☐ Three-digit security code
☐ Debit card number
☐ Personal identification number (PIN)
☐ Cardholder's name
☐ Other personal information, specify:
☐ Unable to provide a description of the personal information affected
Explain:

Individuals affected by the confidentiality incident

Number of individuals affected by the incident:

Number of individuals affected by the incident residing in Quebec:

If possible, break down the number of individuals affected by the incident according to their relationship with the organization, whether they are employees, clients, self-managers, partners, home aides, students, users, members, volunteers, suppliers, etc., current or former:

Incident reporter

First name, last name:

Position:
Communication method (email and/or phone):

ANNEX C: CONFIDENTIALITY DECLARATION

I, the undersigned, declare that I have read Ex aequo's Privacy Protection Policy, and I commit to respecting its terms. I acknowledge and agree that my confidentiality obligation remains even after the termination of the employment, internship, or volunteer relationship with Ex aequo.

Signed at [insert location] on: [insert date]

Name in block letters :

Signature :

ANNEX D: CONFIDENTIALITY INCIDENT: RESPONSE PLAN

Steps to take:

- When an employee or participant notices a confidentiality incident, they communicate with the person responsible for protecting personal information using the designated reporting form.
- The responsible person identifies reasonable measures to reduce the risk of harm and to prevent new incidents.
- The responsible person evaluates whether the incident presents a severe risk of harm, according to the definition in Annex D.
- If the incident presents a severe risk of harm, management immediately notifies the Access to Information Commission (CAI) using the designated form and all individuals whose personal information is affected.
- The responsible person maintains a register of all incidents.
- Management responds to the CAI's request for a copy of the register if necessary.

ANNEX E: CONFIDENTIALITY INCIDENT: CONTENT OF COMMUNICATION TO CONCERNED INDIVIDUALS

When

Article 5.5 of this policy indicates that an organization must notify "with diligence" all individuals whose personal information has been affected by a confidentiality incident. This notice must be sent directly to the individuals concerned. However, the Regulation on Confidentiality Incidents provides situations where communication may exceptionally be made through public notice.

Content

As with the written notice to the CAI, the written notice to the individuals concerned must include the following elements:

- A description of the personal information affected by the incident or, if this information is unknown, the reasons why it is impossible to provide such a description;
- A brief description of the circumstances of the incident;
- The date or period when the incident occurred (or an approximation if this information is unknown);
- A brief description of the measures the organization has taken or intends to take following the incident to reduce the risks of harm;
- The measures the organization suggests the individual concerned take to reduce/mitigate the risks of harm;
- The contact details of the person from whom the individual concerned can obtain more information about the incident.

ANNEX F: CONFIDENTIALITY INCIDENT: SERIOUS RISK OF SIGNIFICANT HARM ASSESSMENT QUESTIONNAIRE

Evaluate if the incident presents a serious risk of harm:

For any confidentiality incident, the organization must assess the severity of the risk of harm to the individuals concerned. To do so, it must consider, among other things:

- What is the sensitivity of the information involved?
- What are the anticipated consequences of its use?
- What is the likelihood that it will be used for harmful purposes?

Sensitive information:

- Financial documents;
- Medical records;
- Personal information commonly communicated is generally not considered sensitive (name, address);
- Except if the context makes it sensitive information: names and addresses associated with specialized periodicals or activities that identify them.

Serious harm:

- Humiliation;
- Damage to reputation or relationships;
- Loss of job or business opportunities or professional activities;
- Financial loss;
- Identity theft;
- Negative effect on credit record;
- Damage to property or loss of property.

To determine the likelihood of misuse:

- What happened, and what are the risks that a person suffers harm from because of the breach?
- Who had access to or could have access to the personal information?
- How long was the personal information exposed?
- Has misuse of the information been observed?
- Has malicious intent been demonstrated (theft, hacking)?
- Was the information exposed to entities or individuals likely to use it to cause harm or who represent a risk to the reputation of the affected individuals?

If the analysis reveals a severe risk of harm, the organization must notify the Commission and the individuals concerned about the incident. Otherwise, it must continue its work to reduce the risks and prevent a similar incident from occurring again.

ANNEX G: Confidentiality incidents register

- Incident:
- Date of the incident:
- Date of detection of the incident by the organization:
- Date of transmission of the reporting form:
- Circumstances of the incident:
- Number of individuals affected:
- Assessment of the severity of the risk of harm:
- Measures taken in response to the incident:

ANNEX H: Consent form

First name:

Last name:

Address:

City:

Postal code:

Phone:

Email:

I hereby freely and knowingly consent to Le service Oxili transmitting my personal information to self-managers, their close caregivers, and their involved interveners in the home support service plans: name, first name, phone number, email address, COVID-19 vaccination status, and if I have allergies to animals.
This personal information will be transmitted to enable the matching of home aides to self-managers and used according to the required security standards.

Signed at [insert location] on: [insert date]

First and last name in block letters:

Signature: