# POLITIQUE DE PROTECTION

# DES RENSEIGNEMENTS PERSONNELS

**ADOPTÉ LE 28 MARS 2024**

## INTRODUCTION

Ex aequo a, à titre d'organisme communautaire en promotion et en défense collective des droits, une politique de confidentialité des renseignements personnels. Il a également une politique de confidentialité des renseignements personnels pour son service Oxili étant donné que celui-ci a des enjeux de confidentialité qui lui sont propres.

Le service Oxili respecte le droit à la vie privée de chaque individu et s'engage à protéger la confidentialité des renseignements personnels recueillis auprès de tous ses usagers et usagères. Ces renseignements sont disponibles seulement aux employéEs d'Ex aequo et aux personnes professionnelles provenant de l'externe dans l'exercice de leurs fonctions respectives pour le service Oxili. Toutes ces personnes doivent au préalable signer la politique de confidentialité.

# 1 DÉFINITIONS

## 1.1 EmployéE

Toute personne qui travaille pour le service Oxili moyennant une rémunération, incluant la direction, ainsi que toutes personnes non rémunérées (bénévole et stagiaire).

## 1.2 Usager et usagère

Toute personne utilisatrice du service Oxili : autogestionnaire, proche aidantE, préposéE et intervenantE du réseau de la santé.

## 1.3 Événement

Tout événement auquel le service Oxili participe ou organise.

## 1.4 Formulaire de signalement

Le formulaire mis à la disposition de tous les usagers et usagères du service Oxili afin d'informer la personne responsable des renseignements personnels.

## 1.5 Incident de confidentialité

Tout accès non autorisé par la loi à un renseignement personnel, à son utilisation ou à sa communication, de même que sa perte ou toute autre forme d'atteinte à sa protection.

## 1.6 Publication

Toute publication produite par le service Oxili ou à laquelle le service Oxili contribue, sous quelque forme que ce soit (verbal, écrit, audio, vidéo, informatisé ou autre).

## 1.7 Registre des incidents de confidentialité

L'ensemble des renseignements consignés sur des incidents déclarés et concernant les circonstances de l'incident, le nombre de personnes visées, l'évaluation de la gravité du risque de préjudice et les mesures prises en réaction à l'incident. Les dates pertinentes y figurent aussi : survenance de l'incident, détection par l'organisation, transmission des avis (s'il y a lieu), etc.

## 1.8 Risque sérieux de préjudices

Le risque évalué à la suite d'un incident de confidentialité qui pourrait porter préjudice aux personnes concernées. Ce risque est analysé par la personne

responsable des renseignements personnels. Pour tout incident de confidentialité, la personne responsable évalue la gravité du risque de préjudice pour les personnes concernées en estimant **«** la sensibilité des renseignements concernés **»**, **«** les conséquences appréhendées de leur utilisation **»** et **«** la probabilité qu'ils soient utilisés à des fins préjudiciables **»**.

### 1.9 Renseignement personnel

Tout renseignement fourni ou communiqué au service Oxili qui concerne un usager ou usagère actuelle ou potentielle et qui peut être utilisé pour l'identifier: son nom, son numéro de téléphone, son adresse, son adresse courriel, son genre, son orientation sexuelle et toute information concernant sa santé. Ces renseignements peuvent être fournis ou communiqués sous quelque support que ce soit (verbal, écrit, audio, vidéo, informatisé ou autre).

Pour plus de certitude :

- Les renseignements qui ne permettent pas d'identifier un individu dans le cadre d'un témoignage ne sont pas des renseignements confidentiels.
- Les données statistiques ne sont pas des renseignements confidentiels puisqu'elles ne permettent pas d'identifier un individu ;
- Les photographies ou enregistrements qui ne permettent pas d'identifier un individu ne constituent pas un renseignement confidentiel relatif à cet individu.

### 1.10 Service ou activité

Tout service que le service Oxili rend à un individu à la demande de celui-ci, ou toute activité à laquelle il participe.

## 2 PHOTOGRAPHIES ET ENREGISTREMENTS

2.1 Tout individu a le choix d'être photographié ou non, ou d'être enregistré (audio/vidéo) ou non.

2.2 Les photographies ou enregistrements qui permettent d'identifier un individu comme employéE d'Ex aequo pour Le service Oxili ne constituent pas un renseignement confidentiel relatif à cet individu.

## 3 OBLIGATION DE CONFIDENTIALITÉ

3.1 Les EmployéEs d'Ex aequo doivent signer une entente de confidentialité avant d'exercer leurs fonctions ou d'exécuter leurs mandats auprès du service Oxili.

3.2 L'obligation de confidentialité s'applique à la durée du bénévolat d'une personne, d'un stage, d'un contrat avec unE professionnelLE ou du lien d'emploi d'unE employéE avec Ex aequo. Cette obligation demeure même après la fin du bénévolat de la personne, de la fin du stage, de la fin du contrat ou du lien d'emploi avec Ex aequo.

## 4 COLLECTE ET USAGE DES RENSEIGNEMENTS PERSONNELS

4.1 Le service Oxili peut, au besoin, constituer un ou des dossiers contenant des renseignements personnels concernant les usagers et usagères. La constitution de tels dossiers a pour objet de :

- maintenir les coordonnées à jour ;
- documenter les profils des usagers et usagères.

4.2 Le service Oxili constitue des dossiers contenant des renseignements personnels concernant les usagers et usagères. La constitution de tels dossiers a pour objet de permettre au service Oxili de fournir des services et parfois réaliser une activité ou une publication.

4.3 Le service Oxili peut seulement recueillir les renseignements personnels qui sont nécessaires aux fins du dossier et peut utiliser les renseignements personnels seulement à ces fins.

4.4 Les renseignements personnels peuvent seulement être recueillis auprès de la personne concernée, à moins que celle-ci consente à ce que la cueillette soit réalisée auprès de son ou sa représentante ou que la loi l'autorise.

## 5 GESTION DES RENSEIGNEMENTS PERSONNELS

5.1 La personne à la direction générale d'Ex aequo est mandatée par le conseil d'administration pour être la personne responsable d'assurer la protection des renseignements personnels. Sur le site web d'Ex aequo, il doit être indiqué que la personne à la direction générale est également la personne responsable, « personne responsable de la protection des renseignements personnels » ainsi que le moyen de la joindre.

La personne responsable s'assure de la tenue d'un Registre des incidents de confidentialité.

5.2 Sous réserve de l'article 5.3, les employéEs sont autoriséEs à accéder à tout renseignement personnel que détient le service Oxili. La direction et une personne professionnelle externe sont autorisées à accéder aux renseignements personnels

dans la mesure où cet accès est nécessaire à la réalisation d'une tâche dans l'exercice de ses fonctions.

5.3 Pour l'application des lois, un **incident de confidentialité** correspond à tout accès, utilisation ou communication non autorisées par la loi d'un renseignement personnel, de même qu'à la perte d'un renseignement personnel ou à toute autre atteinte à sa protection.

5.4 Lorsqu'unE employéE ou un usager ou une usagère constate un incident de confidentialité, il ou elle doit informer avec diligence la personne responsable de la protection des renseignements personnels afin qu'il soit inscrit au Registre. L'employéE, l'usager ou l'usagère doit, pour ce faire, compléter un formulaire de signalement et l'acheminer ensuite à la personne responsable de la protection des renseignements personnels.

Le registre doit conserver les informations sur un incident de confidentialité pour une période de cinq ans.

Doit être colligé dans le formulaire de signalement :

- Une description des renseignements personnels touchés par l'incident ou, si cette information est inconnue, les raisons pour lesquelles il est impossible de fournir une telle description ;
- Une brève description des circonstances de l'incident ;
- La date ou la période à laquelle a eu lieu l'incident (ou une approximation si cette information n'est pas connue) ;
- La date ou la période à laquelle l'organisation s'est aperçue de l'incident ;
- Le nombre de personnes concernées par l'incident (ou une approximation si cette information n'est pas connue).

5.5 La personne responsable juge si l'incident présente un « risque sérieux de préjudice ». Les renseignements ainsi que les mesures à prendre afin de diminuer le risque qu'un préjudice sérieux soit causé aux personnes concernées sont versés au Registre.

Si l'incident présente un risque sérieux de préjudice, la personne responsable avise la Commission d'accès à l'information et les personnes concernées de tout incident présentant un risque sérieux de préjudice à l'aide du formulaire approprié.

## 6 CONSERVATION DES RENSEIGNEMENTS PERSONNELS

6.1 Les employéEs ayant accès aux dossiers en vertu de l'article 5 s'obligent à :

- S'assurer que les renseignements personnels soient gardés à l'abri de tout dommage physique ou d'accès non autorisé;

- S’assurer que tous les documents électroniques comportant des renseignements personnels, incluant ceux copiés sur un appareil de stockage portatif, soient cryptés et protégés par des mots de passe. La gestion des mots de passe se fait selon une méthode éprouvée ;

- Garder les renseignements personnels en format papier dans des classeurs pouvant être verrouillés et s’assurer que les classeurs soient verrouillés à la fin de chaque journée de travail. Les clés des classeurs doivent être gardées dans des endroits sûrs.

6.2 Lorsqu’unE employéE peut également, à certains égards, être qualifiéE d’usager ou d’usagère, les renseignements personnels concernant chaque titre seront conservés séparément.

6.3 Les dossiers des usagers et usagères constitués en vertu de cette politique sont la propriété du service Oxili.

## 7 DESTRUCTION DES RENSEIGNEMENTS PERSONNELS

7.1 Sous réserve de l’article 7.2, les renseignements personnels sont conservés tant et aussi longtemps que l’objet pour lequel ils ont été recueillis n’a pas été modifié, à moins que l’individu concerné ait consenti à ce qu’il en soit autrement. Ces renseignements personnels sont ensuite détruits de façon à ce que les données y figurant ne puissent plus être reconstituées.

7.2 Les dossiers concernant les usagers et usagères sont conservés par Le service Oxili. Les dossiers des préposéEs à domicile avec un statut «définitivement inactifs» depuis 7 ans sont détruits, tandis que les dossiers des autogestionnaires qui deviennent «définitivement inactifs» sont détruits immédiatement.

7.3 Pour plus de certitude, les renseignements confidentiels concernant un individu ayant offert un témoignage, tels que son nom et ses coordonnées, sont détruits une fois le témoignage publié ou diffusé, à moins que l’individu ait préalablement consenti à ce que les renseignements confidentiels le concernant soient conservés pour permettre au service Oxili de le recontacter dans le futur. Pour plus de certitude, chaque utilisation du témoignage d’une personne doit être approuvée par celle-ci.

## 8 DIVULGATION DE RENSEIGNEMENTS PERSONNELS À UN TIERS

8.1 Autre que dans les situations où la loi le requiert et sous réserve des autres dispositions du présent article 8, les renseignements personnels ne peuvent être divulgués à un tiers qu’après l’obtention du consentement verbal ou écrit, manifeste, libre et éclairé de la personne concernée ou de son représentant ou sa représentante. Un tel consentement ne peut être donné que pour une fin spécifique et pour la durée nécessaire à la réalisation de cette dernière.

8.2 Les préposéEs à domiciles devront signer un formulaire de consentement de divulgation des renseignements personnels.

8.2 Les renseignements personnels peuvent être divulgués sans le consentement de la personne concernée si la vie, la santé ou la sécurité de celle-ci est gravement menacée. La divulgation doit alors être effectuée de la façon la moins préjudiciable pour la personne concernée.

8.3 Tel que permis par la loi, le service Oxili peut divulguer des renseignements personnels nécessaires à sa défense ou poursuite intentée contre le service Oxili de la part d'un usager ou d'une usagère ou de l'une de ses personnes héritières, exécutrices testamentaires, ayants droit ou cessionnaires, y compris toute réclamation émanant de l'assureur d'un usager ou d'une usagère.

## 9 COMMUNICATION DE RENSEIGNEMENTS PERSONNELS À LA PERSONNE CONCERNÉE

9.1 Sous réserve de l'article 9.2, les usagers et usagères ont le droit de connaître les renseignements personnels que le service Oxili a reçus, recueillis et conserve à leur sujet, d'avoir accès à de tels renseignements et de demander que des rectifications soient apportées à ceux-ci.

9.2 Le service Oxili doit restreindre l'accès aux renseignements personnels lorsque la loi le requiert ou lorsque la divulgation révélerait vraisemblablement des renseignements confidentiels au sujet d'un tiers.

9.3 Une demande d'un usager et usagère en lien avec l'article 9.1 doit être traitée dans un délai maximal de 30 jours.

## 10 MANQUEMENT À L'OBLIGATION DE CONFIDENTIALITÉ

10.1 UnE employéE manque à son obligation de confidentialité lorsque cette personne :

- Communique des renseignements personnels à des individus n'étant pas autorisés à y avoir accès ;
- Discute de renseignements personnels à l'intérieur ou à l'extérieur des locaux du service Oxili alors que des individus n'étant pas autorisés à y avoir accès sont susceptibles de les entendre ;
- Laisse des renseignements personnels sur papier ou support informatique à la vue dans un endroit où des individus n'étant pas autorisés à y avoir accès sont susceptibles de les voir ;
- Fait défaut de suivre les dispositions de cette politique.

10.2 Advenant un manquement à l'obligation de confidentialité, des mesures disciplinaires appropriées, pouvant aller jusqu'à la résiliation du contrat de service ou de toute autre relation avec le service Oxili, seront prises à l'égard de la partie contrevenante et des mesures correctives seront adoptées au besoin afin de prévenir qu'un tel scénario ne se reproduise.

## 11 RECOURS

11.1 S'il s'avère que les renseignements personnels d'une personne ont été utilisés de façon contraire à une disposition de cette politique, cette personne peut déposer une plainte auprès de la personne responsable des renseignements personnels d'Ex aequo ou auprès du conseil d'administration d'Ex aequo si la plainte concerne la personne à la direction générale.

11.2 Comme prévu par la loi, la personne s'étant vu refuser l'accès ou la rectification des renseignements personnels la concernant peut déposer sa plainte auprès de la Commission d'accès à l'information pour l'examen du désaccord dans les 30 jours du refus d'Ex aequo d'accéder à sa demande ou de l'expiration du délai pour y répondre.

## ANNEXE A : FORMULAIRE DE SIGNALEMENT

Comme prévu dans la Politique de protection des renseignements personnels, vous devez remplir ce formulaire de signalement aussitôt que vous constatez un incident de confidentialité et le remettre à la direction générale.

Les informations colligées seront versées au registre des incidents sur la confidentialité. À partir de ces informations, la direction générale décide si l'incident présente « un risque de préjudice sérieux » pour les personnes concernées et remplit une déclaration à la Commission de l'accès à l'information, si nécessaire. Des mesures pour contrôler et prévenir le type d'incident déclaré seront ensuite déployées.

Un incident de confidentialité correspond à tout accès, utilisation ou communication non autorisés par la loi d'un renseignement personnel, de même qu'à la perte d'un renseignement personnel ou à toute autre atteinte à sa protection.

Par exemple, un incident de confidentialité pourrait se produire lorsque:

- un membre de l'équipe consulte un renseignement personnel sans autorisation;
- un membre de l'équipe communique des renseignements personnels au mauvais destinataire;
- l'organisation est victime d'une cyberattaque : hameçonnage, rançongiciel, etc.

## ANNEXE B : FORMULAIRE DE SIGNALEMENT D'UN INCIDENT DE CONFIDENTIALITÉ (DOCUMENT INTERNE)

**1. Date et période de l'incident de confidentialité**

Date de l'incident :

Date de la découverte de l'incident :

L'incident a eu lieu sur une période de :

**2. Type d'incident de confidentialité (identifier avec un "x" le type d'incident) :**

☐ Accès non autorisé par la loi à un renseignement personnel

☐ Utilisation non autorisée par la loi d'un renseignement personnel

☐ Communication non autorisée par la loi d'un renseignement personnel

☐ Perte d'un renseignement personnel ou toute autre atteinte à la protection d'un tel renseignement

**3. Causes et circonstances de l'incident (identifier avec un "x" les causes ou circonstances) :**

☐ Altération délibérée

☐ Communication accidentelle

☐ Communication délibérée sans autorisation

☐ Consultation non autorisée

☐ Cyberattaque (virus, logiciel espion, etc.)

☐ Défaillance technique

☐ Destruction accidentelle

☐ Destruction volontaire sans autorisation

☐ Divulgation accidentelle

☐ Divulgation délibérée sans autorisation

☐ Erreur humaine

☐ Hameçonnage (phishing)

☐ Ingénierie sociale (technique de manipulation pour obtenir des rens. pers.)

☐ Perte d'accès aux renseignements

☐ Perte de renseignements

☐ Rançongiciel

☐ Utilisation incompatible

☐ Vol de renseignements

☐ Autre, précisez :

**4. Sur quel(s) support(s) les renseignements personnels étaient-ils conservés au moment de l'incident ?**

☐ Ordinateur du bureau

☐ Ordinateur du domicile

☐ Dispositif amovible électronique

☐ Papier

☐ Clé USB

☐ Serveur

☐ CD

☐ Bande sonore

☐ Téléphone portable

☐ Infonuagique (cloud)

☐ Tablette

☐ Vidéosurveillance

☐ Ordinateur portable

☐ Photo

☐ Autre, précisez :

**5. Identification des renseignements personnels visés par l'incident de confidentialité (identifier avec un x pour chaque renseignement).**

☐ Nom

☐ Prénom

☐ Adresse du domicile

☐ Date de naissance

☐ Numéro de téléphone au domicile

☐ Numéro du cellulaire

☐ Adresse courriel personnelle

☐ Numéro de permis de conduire

☐ Numéro d'assurance sociale

☐ Numéro d'assurance maladie

☐ Numéro de passeport

☐ Salaire Fonction / occupation

☐ Renseignements sur des employés, ou bénéficiaires

☐ Renseignements médicaux

☐ Renseignements génétiques

☐ Renseignements scolaires / académiques

☐ Renseignements bancaires / numéro de compte / institution / placements / hypothèque

☐ Numéro de carte de crédit

☐ Numéro d'identification personnel (NIP)

☐ Nom du détenteur

☐ Code de sécurité à trois chiffres

☐ Numéro de carte de débit

☐ Numéro d'identification personnel (NIP)

☐ Nom du détenteur

☐ Autres renseignements personnels, précisez :

☐ Impossible de fournir une description des renseignements personnels visés

Expliquez :

**6. Personnes concernées par l'incident de confidentialité**

Nombre de personnes concernées par l'incident :

Nombre de personnes concernées par l'incident qui résident au Québec :

Si possible, ventilez le nombre de personnes concernées par l'incident selon leur lien avec l'organisation, qu'il s'agisse d'employéEs, de clientEs, autogestionnaires, partenaires, préposéEs à domicile, d'étudiantEs, d'usagers et d'usagères, de membres, de bénévoles, de fournisseurs, etc., actuelLEs ou ancienNEs :

**7. Personne déclarant l'incident**

Prénom, nom de la personne :

Fonction :
Moyen de communication (courriel et / ou téléphone)

## ANNEXE C: DÉCLARATION RELATIVE À LA CONFIDENTIALITÉ

Je, soussignéE déclare avoir lu la Politique de protection des renseignements personnels d'Ex aequo et je m'engage à en respecter les termes. Je reconnais et accepte que mon obligation de confidentialité demeure même après que le lien d'emploi, de stage ou de bénévolat avec Ex aequo soit rompu.

Signé à [inscrivez le lieu] le : [inscrivez la date]

Nom en lettres moulées :

Signature :

## ANNEXE D : INCIDENT DE CONFIDENTIALITÉ : PLAN DE RÉPONSE

### Démarches à effectuer

Lorsqu'unE employéE ou participantE constate un incident de confidentialité, il ou elle communique avec la personne responsable de la protection des renseignements personnels par le biais d'un formulaire de signalement prévu à cette fin.

La personne responsable identifie les mesures raisonnables pour réduire le risque de préjudice et pour prévenir de nouveaux incidents.

La personne responsable évalue si l'incident présente un risque de préjudice sérieux, selon la définition présentée à l'annexe D.

Dans le cas où l'incident présente un risque de préjudice sérieux, la direction prévient sans délai la Commission d'accès à l'information (CAI) via le formulaire prévu à cette fin et toute personne dont les renseignements personnels sont affectés.

La personne responsable tient un registre de tous les incidents.

La direction répond à la demande de la CAI d'avoir une copie du registre, le cas échéant.

## ANNEXE E : INCIDENT DE CONFIDENTIALITÉ : CONTENU DE LA COMMUNICATION AUX PERSONNES CONCERNÉES

### Quand

Tel qu'indiqué à l'article 5.5 de la présente politique, un organisme doit aviser « avec diligence » toutes les personnes dont les renseignements personnels ont été touchés par un incident de confidentialité. Cet avis doit être envoyé directement aux personnes concernées. Toutefois, le **Règlement sur les incidents de confidentialité** prévoit des situations où la communication peut se faire exceptionnellement par le biais d'un avis public.

### Contenu

Comme c'est le cas pour l'avis écrit à la CAI, l'avis écrit aux personnes concernées doit contenir les éléments suivants :

- Une description des renseignements personnels touchés par l'incident ou, si cette information est inconnue, les raisons pour lesquelles il est impossible de fournir une telle description ;
- Une brève description des circonstances de l'incident ;
- La date ou la période à laquelle a eu lieu l'incident (ou une approximation si cette information n'est pas connue) ;
- Une brève description des mesures que l'organisme a prises ou entend prendre suivant l'incident dans le but de réduire les risques de préjudice ;
- Les mesures que l'organisme suggère à la personne concernée de prendre dans le but de réduire/atténuer les risques de préjudice ;
- Les coordonnées de la personne auprès de laquelle la personne concernée peut obtenir de plus amples renseignements à propos de l'incident.

## ANNEXE F : INCIDENT DE CONFIDENTIALITÉ : QUESTIONNAIRE D'ÉVALUATION DU « RISQUE SÉRIEUX DE PRÉJUDICE GRAVE »

### Évaluer si l'incident présente un risque de préjudice sérieux[1]

Pour tout incident de confidentialité, l'organisation doit évaluer la gravité du risque de préjudice pour les personnes concernées. Pour ce faire, elle doit considérer, entre autres :

- Quelle est la **sensibilité** des renseignements concernés ?
- Quelles sont les **conséquences appréhendées** de leur utilisation ?
- Quelle est la probabilité qu'ils soient utilisés à des **fins préjudiciables ?**

### 1. Renseignements sensibles

- Documents financiers ;
- Dossiers médicaux ;
- Les renseignements personnels que l'on communique de manière courante ne sont généralement pas considérés comme sensibles (nom, adresse) ;
- Sauf si le contexte en fait des renseignements sensibles : nom, adresses associéES à des périodiques spécialisés ou à des activités qui les identifient.

### 2 Préjudice grave

- Humiliation ;
- Dommage à la réputation ou aux relations ;
- Perte de possibilité d'emploi ou d'occasion d'affaires ou d'activités professionnelles ;
- Perte financière ;

---

[1] [1] Le questionnaire respecte le **Règlement sur les incidents de confidentialité**

Note : le Commissariat à la protection de la vie privée du Canada a produit une vidéo d'aide à l'évaluation : https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/protection-des-renseignements-personnels-pour-les- entreprises/mesures-de-securite-et-atteintes/atteintes-a-la-vie-privee/comment-reagir-a-une-atteinte-a-la-vie-privee-dans- votre-entreprise/atteinte_101/atteinte_risques/

- Vol d’identité ;
- Effet négatif sur le dossier de crédit ;
- Dommage aux biens ou leur perte ;

**3 Pour déterminer la probabilité d’un mauvais usage**

- Qu’est-il arrivé et quels sont les risques qu’une personne subisse un préjudice en raison de l’atteinte ?
- Qui a eu accès aux renseignements personnels ou aurait pu y avoir accès ?
- Combien de temps les renseignements personnels ont-ils été exposés ?
- A-t-on constaté un mauvais usage des renseignements ?
- L’intention malveillante a-t-elle été démontrée (vol, piratage) ?
- Les renseignements ont-ils été exposés à des entités ou à des personnes susceptibles de les utiliser pour causer un préjudice ou qui représentent un risque pour la réputation de la ou des personnes touchées ?

Si l’analyse fait ressortir un risque de préjudice sérieux, l’organisation doit aviser la Commission et les personnes concernées de l’incident. Dans le cas contraire, elle doit tout de même poursuivre ses travaux pour réduire les risques et éviter qu’un incident de même nature se produise à nouveau.

## ANNEXE G : REGISTRE DES INCIDENTS DE CONFIDENTIALITÉ

**Incident**

Date de l’incidence

Date de détection de l’incident par l’organisation

Date de transmission du formulaire de signalement

Circonstance de l’incident

Nombre de personnes visées

Évaluation de la gravité du risque de préjudice

Mesures prises en réaction de l’incident

## ANNEXE H : FORMULAIRE DE CONSENTEMENT

Prénom :

Nom :

Adresse :

Ville : Code postal :

Téléphone :

Courriel :

Par la présente, je consens de façon libre et éclairée à ce que Le service Oxili transmette aux autogestionnaires, à leurs proches-aidantEs et à leurs intervenantEs impliquéEs dans les plans de service de soutien à domicile mes renseignements personnels suivants : nom, prénom, numéro de téléphone, adresse courriel, statut vaccinal de la COVOD-19 et si j'ai des allergies aux animaux.

La transmission de ces renseignements personnels a pour but de permettent le jumelage des aides à domicile aux autogestionnaires. Ces renseignements seront utilisés selon les normes de sécurité requises.

Signé à [inscrivez le lieu] le : [inscrivez la date]

Prénom et nom en lettres moulées :

Signature :