POLITIQUE DE CONFIDENTIALITÉ - Mars 2024
Coalition des Tables Régionales d'Organismes Communautaires

Politique de confidentialité relative aux renseignements personnels de la CTROC.

À partir de la politique de confidentialité du COCQ-SIDA et du RQ-ACA

Adoptée le 6 mars 2024 par le conseil d'administration

La Coalition des Tables Régionales d'Organismes Communautaires

Préambule

Protéger les renseignements personnels de chacune, sans compromis ! *Vers un idéal, où les renseignements personnels appartiennent exclusivement aux personnes concernées.*

La présente politique précise les droits et les obligations des membres de l'équipe de travail et de la Coalition des Tables Régionales d'Organismes Communautaire (CTROC), en vertu des droits conférés par les articles 35 à 40 du Code civil en matière de protection des renseignements personnels, des règles particulières à l'égard des renseignements personnels sur autrui qu'une personne recueille, détient, utilise ou communique à des tiers à l'occasion de l'exploitation d'une entreprise au sens de l'article 1525 du Code civil.

Cette politique de protection des renseignements personnels vise non seulement à protéger largement l'intégrité des membres de l'équipe de travail de la CTROC, mais aussi à instaurer de meilleures pratiques dans une vision rigoureuse et de confiance.

Dans un contexte où les renseignements personnels sont de plus en plus accessibles et même compris comme une marchandise, nous souhaitons que cette politique soit intégrante et que sa portée permette de revisiter et d'établir des pratiques évolutives. Ces dernières ont pour vision de permettre à toute l'équipe de s'éduquer et se défendre face à ses propres droits.

Elle s'inspire des travaux effectués par la COCQ-SIDA et remercie l'organisme de son temps et dévouement auprès du milieu communautaire autonome pour ce dossier.

Politique de confidentialité relative aux renseignements personnels

La Coalition des Tables Régionales d'Organismes Communautaire (CTROC) respecte le droit à la vie privée de chaque individu et s'engage à protéger la confidentialité des renseignements confidentiels recueillis auprès de son personnel et de ses membres. En règle générale, les renseignements confidentiels sont disponibles seulement aux personnes qui doivent y avoir accès dans l'exercice de leurs fonctions au sein de la CTROC.

La présente politique s'applique à l'ensemble du personnel de la CTROC, que ce soit sur une base régulière ou temporaire, que les personnes fassent partie de l'équipe de la permanence ou qu'elles soient employées sur un projet en particulier. Dans le cas échéant, elle s'applique également aux potentiels stagiaires et bénévoles qui œuvrent au sein de l'organisme.

Elle a pour objet d'établir, en matière de protection des renseignements personnels, des règles particulières, à l'égard des renseignements personnels sur autrui qu'une personne recueille, détient, utilise ou communique à des tiers.

Le transfert des renseignements personnels s'applique à tous types de communications, incluant les réseaux sociaux et les discussions informelles.

1. Définitions

Employé.e.s
Toute personne qui travaille pour la CTROC, incluant le conseil d'administration.

Formulaire de signalement
Le formulaire de signalement est à la disposition de toutes les employé.e.s, dans le but d'informer la personne responsable d'un incident de confidentialité.

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.

Publication
Toute publication produite par la CTROC ou à laquelle la CTROC contribue, quelle qu'en soit la forme (verbale, écrite, audio, vidéo, informatisée ou autre).

Registre des incidents sérieux

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.

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. 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 ».

Renseignement personnel

Tout renseignement fourni ou communiqué à la CTROC sous quelque support que ce soit (verbal, écrit, audio, vidéo, informatisé ou autre) et qui peut être utilisé pour l'identifier, y compris : son nom, son numéro de téléphone, son adresse, son courriel, son genre, son orientation sexuelle et toute information concernant sa santé.

2. Obligation de confidentialité

2.1. Toutes les employé.e.s sont tenues de signer la présente entente de confidentialité (Annexe A) avant d'exercer leurs fonctions ou d'exécuter leurs mandats auprès de la CTROC.

2.2. L'obligation de confidentialité s'applique à la durée de la relation d'un.e employé.e avec la CTROC et persiste à la fin de cette relation.

3. Photographie ou enregistrement

3.1. Toute personne a le droit de refuser d'apparaître sur une photo ou sur un enregistrement vidéo ou audio.

3.2. Les photographies ou enregistrements qui permettent d'identifier un individu comme employé.e de la CTROC ne constituent pas un renseignement confidentiel relatif à cet individu.

L'encadrement applicable à la collecte, la conservation et à la destruction des renseignements personnels

4. Collecte de renseignement personnels

4.1. La personne responsable des dossiers des employé.e.s peut, si nécessaire, constituer des dossiers sur les employé.e.s contenant des renseignements personnels. La constitution de tels dossiers a pour objectif :

- Le maintien des coordonnées à jour;
- Documenter l'expérience de travail;
- Permettre dans le cas des employé.e.s, la réalisation des tâches administratives requises ou permises par la loi.

4.2. Les renseignements personnels peuvent être recueillis seulement auprès de la personne concernée, à moins du consentement de celle-ci, ou s'ils sont prescrit par la loi.

5. La gestion des renseignements personnels

La personne occupant le poste d'agent de communication est désignée responsable de la protection des renseignements personnels de la CTROC. Ainsi, elle est identifiée comme *responsable de la protection des renseignements personnels*, en plus du titre de son poste habituel sur le site de la CTROC. Les moyens pour contacter cette personne sont également disponibles à cet endroit.

La personne responsable de la protection des renseignements personnels peut déléguer cette fonction par écrit, en tout ou en partie, à toute personne.

C'est également elle qui tient le Registre des incidents de confidentialité.

5.1. Lorsqu'un.e employé.e constate un incident de confidentialité, cette personne doit informer avec diligence la personne responsable de la protection des renseignements personnels afin qu'il soit inscrit au Registre. L'employé.e doit, pour ce faire, compléter un formulaire de signalement et l'acheminer ensuite à la personne responsable.

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).

5.2. La personne responsable réunit le conseil d'administration ou consulte ses membres disponibles afin de juger 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.

La personne responsable, en collaboration avec le conseil d'administration, décide d'aviser la Commission d'accès à l'information et les personnes concernées de tout incident présentant un risque sérieux de préjudice.

6. La conservation des renseignements confidentiels

Les employé.e.s ayant accès aux dossiers en vertu de l'article 5.2. s'obligent à :

6.1. S'assurer que les renseignements confidentiels soient gardés à l'abri de tout dommage physique ou accès non autorisé ;

6.2. S'assurer que tous les documents électroniques comportant des renseignements confidentiels, incluant ceux copiés sur un appareil de stockage portatif, soient cryptés et protégés par des mots de passe. Ces mots de passe doivent être modifiés deux fois par année, ainsi qu'à chaque fois que les personnes ayant accès aux dossiers concernés sont remplacées ;

6.3. Garder les renseignements confidentiels 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.

6.4. Les dossiers constitués sur les employé.e.s sont la propriété et sont conservés par la CTROC.

7. Destruction des renseignements personnels

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

7.2. Les dossiers concernant les employées sont conservés par la CTROC.

8. Divulgation d'un renseignement à une tierce personne

8.1. Autre que dans les situations où la loi le requiert et sous réserve des autres dispositions du présent article 8, les renseignements confidentiels ne peuvent être divulgués qu'après l'obtention du consentement écrit, manifeste,

libre et éclairé de la personne concernée. 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 renseignements confidentiels 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, la CTROC peut divulguer des renseignements confidentiels nécessaires à sa défense ou celle de ses employé.e.s, contre toute réclamation ou poursuite intentée contre la CTROC ou ses employé.e.s, y compris toute réclamation émanant de l'assureur d'un.e employé.e.

9. Communication de renseignements confidentiels à la personne concernée

9.1. Sous réserve de l'article 9.2, les employé.e.s ont le droit de connaître les renseignements confidentiels que la CTROC a reçus, recueillis et conservés à leur sujet, d'avoir accès à de tels renseignements.

9.2. La CTROC doit restreindre l'accès au 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 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. Un.e employé.e 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 confidentiels à l'intérieur ou à l'extérieur de la CTROC alors que des individus n'étant pas autorisés à y avoir accès sont susceptibles de les entendre ;
- Laisse des renseignements personnels sur support papier ou 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 travail selon le manuel des conditions de travail en vigueur à la CTROC ou de toute autre relation avec la CTROC, seront prises à l'égard de la partie contrevenante et des mesures correctives seront adoptées au besoin afin de prévenir qu'une telle situation 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 ou auprès du conseil d'administration de la CTROC, si la plainte concerne la personne responsable.

11.2. Comme prévu par la loi, la personne dont la plainte concerne une demande d'accès ou de 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 de la CTROC d'accéder à sa demande ou de l'expiration du délai pour y répondre.

DÉCLARATION RELATIVE À LA CONFIDENTIALITÉ

Je, soussigné·e, déclare avoir lu la Politique de confidentialité da la CTROC et m'engage à en respecter les termes. Je reconnais et accepte que mon obligation de confidentialité soit maintenue à la fin de mon emploi, stage ou bénévolat auprès de la CTROC.

Signé à _____ le :

Nom en lettres moulées :

La Coalition des Tables Régionales d'Organismes Communautaires

Incident de confidentialité
Plan de réponse

Démarches à effectuer

1- Lorsqu'un.e employé.e constate un incident de confidentialité, cette personne communique avec la personne responsable par le biais d'un formulaire de signalement prévu à cette fin.
2- La personne responsable, en collaboration avec le conseil d'administration, identifient les mesures raisonnables pour réduire le risque de préjudice et pour prévenir de nouveaux incidents.
3- La personne responsable, en collaboration avec le conseil d'administration, évaluent si l'incident présente un risque de préjudice sérieux?
4- Dans le cas où l'incident présente un risque de préjudice sérieux, la personne responsable, 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.
5- La personne responsable tient un registre de tous les incidents.
6- La personne responsable répond à la demande de la CAI d'avoir une copie du registre, le cas échéant.

INCIDENT DE CONFIDENTIALITÉ CONTENU DE LA COMMUNICATION AUX PERSONNES CONCERNÉES

Quand

Le **Règlement sur les incidents de confidentialité** stipule aussi qu'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, à moins qu'un tel avis ne leur cause un préjudice additionnel ou ne nuise à l'organisme et/ou si l'organisme ne possède pas les coordonnées de la personne. Le cas échéant, l'organisme peut aviser les personnes concernées au moyen d'un avis public.

Contenu

Comme c'est le cas pour l'avis écrit à la Commission d'accès à l'information (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 suite à 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.

INCIDENT DE CONFIDENTIALITÉ QUESTIONNAIRE D'ÉVALUATION DU « RISQUE SÉRIEUX DE PRÉJUDICE GRAVE »

Évaluer si l'incident présente un risque de préjudice sérieux

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, notamment :

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

1. Renseignement 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 ;
- Vol d'identité ;
- Effet négatif sur le dossier de crédit ;
- Dommage aux biens ou à 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.