Concertation régionale des
organismes communautaires
de l'Abitibi-Témiscamingue

POLITIQUE DE GESTION DES RENSEIGNEMENTS PERSONNELS

Adopté en CA le 16 avril 2024

TABLE DES MATIÈRES

La présente *Politique de gestion des renseignements personnels* a pour but de vous aider à comprendre nos pratiques en matière de cueillette, d'utilisation, de divulgation et de conservation des renseignements personnels. En nous fournissant des renseignements personnels, vous acceptez que ceux-ci soient traités conformément à ce qui est indiqué dans la présente politique, et vous autorisez la Concertation régionale des organismes communautaires de l'Abitibi-Témiscamingue (CROC-AT), ses tiers et ses fournisseurs de services à traiter vos renseignements personnels dans l'exercice de leurs fonctions.

La présente politique sur la protection des renseignements personnels ne s'applique pas aux sites Web de tiers auxquels il est possible d'accéder en cliquant sur des liens qui se trouvent sur le présent site Web, et la CROC-AT n'est nullement responsable à l'égard de tels sites Web de tiers.

DÉFINITIONS

« Date de fermeture de dossier ou d'un fichier »
La date à laquelle le responsable d'un dossier a déterminé que le dossier ou le fichier est terminé et à partir de laquelle il détermine la destruction du dossier.

« Date de destruction du dossier ou d'un fichier »
La date à partir de laquelle un dossier peut être détruit.

« Dossier ou fichier »
Un document ou dossier informatique ou matériel pouvant contenir des renseignements personnels.

« Employé·e »
Toute personne qui travaille pour la CROC-AT moyennant rémunération, incluant la coordination, ainsi que toutes personnes non rémunérées (administrateurs, stagiaires, bénévoles).

« Événement »
Tout événement que la CROC-AT gère ou organise.

« Formulaire de signalement »
Un formulaire signalant mis à la disposition de tout·e employé·e ou participant·e afin d'informer la personne responsable des renseignements personnels 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.

« Participant·e »
Tout individu qui fournit des renseignements personnels à la CROC-AT en lien avec la réalisation d'un événement, la création d'une publication, la participation à une activité ou pour l'obtention d'un service.

« Publication »
Toute publication produite par la CROC-AT ou à laquelle la CROC-AT contribue, sous quelque forme que ce soit (verbal, écrit, audio, vidéo, informatisé, etc.).

« Registre des incidents de confidentialité »
L'ensemble des incidents de confidentialité dont la CROC-AT a fait l'objet, même de ceux qui ne présentent pas un risque de préjudice sérieux pour les personnes.

« Risque sérieux de préjudices »
L'évaluation du risque à la suite d'un incident de confidentialité qui pourrait porter préjudice aux personnes concernées.

« Renseignement personnel »
Tout renseignement fourni ou communiqué à la CROC-AT sous quelque support que ce soit (verbal, écrit, audio, vidéo, informatisé, etc.) qui concerne un·e participant·e ou un.e employé·e et qui peut être utilisé pour l'identifier, y compris :

- La race, l'origine ethnique, la religion, l'orientation sexuelle, l'identité de genre, l'état matrimonial et le niveau d'instruction
- L'adresse électronique personnelle, les messages de courriel et l'adresse IP (protocole Internet-cookie)
- L'âge, la taille, le poids, les dossiers médicaux, le groupe sanguin, l'ADN, les empreintes digitales et la signature vocale
- Les revenus, les achats, les habitudes de consommation, les renseignements bancaires, les données sur les cartes de crédit ou de débit, les rapports de prêt ou de solvabilité et les déclarations de revenus
- Le numéro d'assurance sociale (NAS) ou d'autres numéros d'identification

Certains renseignements permettant d'identifier directement des personnes sont publics. Les renseignements concernant l'exercice d'une fonction d'une personne au sein d'un organisme communautaire sont publics et ne sont pas soumis aux lois protégeant les renseignements personnels, dont le nom, le titre, la fonction, le courriel, l'adresse et le numéro de téléphone de son lieu de travail.

« Service ou activité »
Tout service que la CROC-AT rend à un individu à la demande de celui-ci, ou toute activité à laquelle il participe.

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 employé.e de la CROC-AT ne constituent pas un renseignement personnel relatif à cet individu.

OBLIGATION DE CONFIDENTIALITÉ

3.1
Les employé·es sont tenu·es de signer l'entente de confidentialité[1] avant d'exercer leurs fonctions ou d'exécuter leurs mandats auprès de la CROC-AT.

3.2
L'obligation de confidentialité s'applique à la durée de la relation d'un·e employé·e avec la CROC-AT et survit à la fin de cette relation.

COLLECTE ET USAGE DES RENSEIGNEMENTS PERSONNELS

4.1
La CROC-AT peut, au besoin, monter un ou des dossiers contenant des renseignements personnels concernant les employé·es. La constitution de tels dossiers a pour objet de :

- maintenir les coordonnées à jour ;
- documenter des situations de travail ou d'implication ;
- permettre, dans le cas des employé·es rémunéré·es, la réalisation des tâches administratives requises ou permises par la loi (impôt sur le revenu, assurances collectives, etc.).

4.2
La CROC-AT peut, au besoin, monter un ou des dossiers contenant des renseignements personnels concernant les participants·es. La constitution de tels dossiers a pour objet de permettre à la CROC-AT de réaliser un événement, une publication, de réaliser une activité ou de fournir un service.

4.3
La CROC-AT 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
La personne qui recueille des renseignements personnels sur autrui doit les recueillir auprès de la personne concernée, à moins que celle-ci ne consente à la cueillette auprès de tiers. Toutefois, elle peut, sans le consentement de la personne concernée, recueillir ces renseignements auprès d'un tiers si la loi l'autorise.

GESTION DES RENSEIGNEMENTS PERSONNELS

5.1
La coordination, comme personne exerçant la plus haute autorité dans l'organisation, est la personne responsable d'assurer la protection des renseignements personnels. La coordination peut déléguer cette responsabilité par écrit. Le titre et les coordonnées de la personne responsable de la protection des renseignements personnels sont publiés sur le site Internet de la CROC-AT. La personne responsable s'assure de la tenue d'un Registre des incidents de confidentialité[2].

5.2
La personne responsable est autorisée à accéder à tout renseignement personnel que détient la

[1] Annexe A
[2] Annexe B

CROC-AT. Les autres employé·es sont autorisé·es à accéder aux renseignements personnels dans la mesure où cet accès est nécessaire à la réalisation d'une tâche dans l'exercice de leurs fonctions.

5.3

Pour l'application des lois, un incident de confidentialité correspond à tout accès, utilisation ou communication non autorisé·es 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'un·e employé·e ou un·e participant·e 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 des incidents de confidentialité. L'employé·e ou le/la participant·e doit, pour ce faire, remplir un formulaire de signalement[3] et l'acheminer à la personne responsable de la protection des renseignements personnels. Le formulaire de signalement doit être conservé pour une période de cinq (5) ans.

5.5

La personne responsable de la protection des renseignements personnels et le comité concerné jugent si l'incident présente un « risque sérieux de préjudice »[4]. Les renseignements ainsi que les mesures à prendre afin de diminuer le risque qu'un préjudice sérieux soit causé aux personnes concernées sont inscrits au Registre des incidents de confidentialité.

Si l'incident présente un risque sérieux de préjudice, la personne responsable avise la Commission d'accès à l'information[5] et les personnes concernées[6].

5.6

Chaque employé.e de la CROC-AT est autorisé à accéder aux renseignements personnels que la CROC-AT détient en toute diligence.

CONSERVATION DES RENSEIGNEMENTS PERSONNELS

6.1

Les employé·es ayant accès aux dossiers s'obligent à :

- S'assurer que les renseignements personnels sont gardés à l'abri de tout dommage physique ou accès non autorisé ;
- S'assurer que tous les documents électroniques comportant des renseignements personnels, incluant ceux copiés sur un appareil de stockage portatif, sont protégés par des mots de passe. Ces mots de passe doivent être modifiés chaque fois que les personnes ayant accès aux dossiers concernés sont remplacées ;
- Garder les renseignements personnels en format papier dans des classeurs pouvant être verrouillés, verrouillés les classeurs à la fin de chaque journée de travail et gardées les clés des classeurs dans des endroits sûrs.

[3] Annexe C
[4] Annexe D
[5] Annexe E
[6] Annexe F

6.2
Les dossiers constitués en vertu de cette politique sont la propriété de la CROC-AT.

DESTRUCTION DES RENSEIGNEMENTS PERSONNELS

7.1
Les renseignements personnels sont conservés 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 personnels sont ensuite détruits de façon que les données y figurant ne puissent plus être reconstituées. La date de destruction pour la plupart des dossiers doit être de sept (7) ans après la date de fin du service.

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 de la présente *Loi sur la protection des renseignements personnels dans le secteur privé*, les renseignements personnels ne peuvent être divulgués à un tiers 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 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, la CROC-AT peut divulguer des renseignements personnels nécessaires à sa défense ou celle de ses employé·es contre toute réclamation ou poursuite intentée contre la CROC-AT ou ses employé·es, par ou de la part d'un·e participant·e, d'un·e employé·e, ou de l'une de ses personnes héritières, exécutrices testamentaires, ayants droit ou cessionnaires, y compris toute réclamation émanant de l'assureur d'un·e participant·e ou d'un·e employé·e.

COMMUNICATION DE RENSEIGNEMENTS PERSONNELS À LA PERSONNE CONCERNÉE

9.1
Les participant·es et employé·es ont le droit de connaître les renseignements personnels que la CROC-AT a reçus, recueillis et conservés à leur sujet, d'avoir accès à de tels renseignements et de demander que des rectifications soient apportées à ceux-ci.

9.2
La CROC-AT doit restreindre l'accès aux renseignements personnels lorsque la loi le requiert ou lorsque la divulgation révélerait vraisemblablement des renseignements personnels au sujet d'un tiers.

9.3
Une demande d'un·e participant·e ou d'un·e employé·e doit être traitée dans un délai de 30 jours.

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 personnels à l'intérieur ou à l'extérieur de la CROC-AT 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 travail ou de toute autre relation avec la CROC-AT seront prises à l'égard de la partie contrevenante et des mesures correctives seront adoptées au besoin afin de prévenir qu'un tel scénario se reproduise.

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 coordination de la CROC-AT, ou auprès du conseil d'administration de la CROC-AT si la plainte concerne la coordination.

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 de la CROC-AT d'accéder à sa demande ou de l'expiration du délai pour y répondre.

Adoptée par le Conseil d'administration de la CROC-AT le 16 avril 2024

Annexe A : DÉCLARATION RELATIVE À LA CONFIDENTIALITÉ

Je, soussigné·e, déclare avoir lu la Politique de gestion des renseignements personnels de la CROC-AT et m'engage à en respecter les termes. Je reconnais et accepte que mon obligation de confidentialité survit à la fin de mon emploi, stage ou implication auprès de la CROC-AT.

Signé à _____, le _____

_____	_____
Nom en lettres moulées	Signature

Annexe B : REGISTRE DES INCIDENTS DE CONFIDENTIALITÉ

(Ce formulaire est un modèle établi par le gouvernent du Québec.)

NUMÉRO DE L'INCIDENT :

RENSEIGNEMENTS VISÉS PAR L'INCIDENT : Décrire les renseignements personnels visés par l'incident ou en dresser une liste. Si cette information n'est pas connue, il faut le préciser et expliquer la raison qui justifie l'impossibilité de fournir une telle description.

CIRCONSTANCES DE L'INCIDENT : Décrire brièvement les circonstances de l'incident.

DATE OU PÉRIODE DE L'INCIDENT : Mentionner la date ou la période où l'incident a eu lieu ou, si cette dernière n'est pas connue, une approximation.

DATE OU PÉRIODE DE LA PRISE DE CONNAISSANCE DE L'INCIDENT : Mentionner la date ou la période au cours de laquelle l'organisation a pris connaissance de l'incident.

NOMBRE DE PERSONNES CONCERNÉES PAR L'INCIDENT : Mentionner le nombre de personnes concernées par l'incident ou, si ce dernier n'est pas connu, une approximation.

RISQUE QU'UN PRÉJUDICE SÉRIEUX SOIT CAUSE : OUI ☐ NON ☐ Décrire les éléments qui amènent l'organisation à conclure qu'il existe ou non un risque qu'un préjudice sérieux soit causé aux personnes concernées.

TRANSMISSION DES AVIS À LA COMMISSION D'ACCÈS À L'INFORMATION ET AUX PERSONNES CONCERNÉES :
Date(s) de l'avis à la Commission d'accès à l'information : S'il y a un risque qu'un préjudice sérieux soit causé, inscrire la ou les dates. Sinon, inscrire « Sans objet ».
Date(s) de l'avis aux personnes concernées : S'il y a un risque qu'un préjudice sérieux soit causé, inscrire la ou les dates. Sinon, inscrire « Sans objet ».
Avis public : OUI ☐ NON ☐
Raison : Si un avis public a été diffusé, en expliquer la raison. Dans le cas contraire, inscrire « Sans objet ».

DESCRIPTION DES MESURES PRISES PAR L'ORGANISATION : Décrire brièvement les mesures prises par l'organisation, à la suite de la survenance de l'incident, afin de diminuer les risques qu'un préjudice soit causé.

Annexe C : FORMULAIRE DE SIGNALEMENT D'UN INCIDENT DE CONFIDENTIALITÉ

Vous devez remplir ce formulaire de signalement[7] aussitôt que vous constatez un incident de confidentialité et le remettre à la personne responsable.

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.

1. Date et période de l'incident de confidentialité

Date de l'incident : _____
Date de la découverte de l'incident : _____

2. Type d'incident de confidentialité :

☐ 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 tout autre atteinte à la protection d'un tel renseignement.

3. Causes et circonstances de l'incident :

☐ 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
☐ Hameçonnage (phishing)
☐ Ingénierie sociale (technique de manipulation pour obtenir des renseignements personnels)
☐ Perte d'accès aux renseignements
☐ Perte de renseignements
☐ Rançongiciel
☐ Utilisation incompatible
☐ Vol de renseignements
☐ autres, précisez : _____
_____

[7] Références

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

- ☐ Ordinateur de bureau
- ☐ 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 :

- ☐ 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 de carte de crédit
  - ☐ Code de sécurité à trois chiffres
- ☐ Numéro de carte de débit
  - ☐ Numéro d'identification personnel (NIP)
  - ☐ Nom du détenteur de carte de débit
- ☐ Autres, 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 : _____

Si possible, ventilez le nombre de personnes concernées par l'incident selon leur lien avec l'organisation, qu'il s'agisse d'employés, de stagiaire, de membres, de bénévoles, de fournisseurs, etc., actuels ou anciens : _____ _____ _____

7. Personne déclarant l'incident

Prénom, nom de la personne : _____
Fonction : _____
Signature : _____

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

Évaluer si l'incident présente un risque de préjudice sérieux[8]

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. Renseignements sensibles

- Documents financiers ;
- Dossiers médicaux ;
- Les renseignements personnels que l'on communique de manière courante ne sont généralement pas considérés comme sensibles tels que le nom et l'adresse d'une personne. Toutefois, selon le contexte, tout renseignement peut devenir sensible (ex. les nom et adresse des abonnés de certaines revues spécialisées).

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 ?

[8] Réf : **Règlement sur les incidents de confidentialité** et vidéo d'aide à l'évaluation.

Annexe E : INCIDENT DE CONFIDENTIALITÉ : « FORMULAIRE DÉCLARATION D'UN INCIDENT DE CONFIDENTIALITÉ »

(Ce formulaire est établi par la Commission d'accès à l'information du Québec.)

Annexe F : INCIDENT DE CONFIDENTIALITÉ : CONTENU DE LA COMMUNICATION AUX PERSONNES CONCERNÉES

Quand

Comme 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, dont lorsque le fait de transmettre l'avis est susceptible de représenter une difficulté excessive pour l'organisme ou d'accroître le préjudice causé aux personnes concernées.

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.

PROCÉDURE EN CAS D'INCIDENT DE CONFIDENTIALITÉ

Démarches à effectuer

1. Lorsqu'un·e employé·e ou participant·e constate un incident de confidentialité, il ou elle communique avec la personne responsable par le biais d'un formulaire de signalement prévu à cette fin (annexe C).
2. La personne responsable identifie les mesures raisonnables pour réduire le risque de préjudice et pour prévenir de nouveaux incidents.
3. La personne responsable évalue si l'incident présente un risque de préjudice sérieux, selon la définition présentée à l'annexe E.
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 en annexe E 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.

NOTE :

La Loi sur le privé s'appuie sur l'article 1525 du Code civil pour déterminer la définition d'une entreprise. Selon cette loi, la CROC-AT est considérée comme une entreprise[9]. Elle est donc soumise à la Loi sur la protection des renseignements personnels dans le secteur privé.

[9] https://www.cai.gouv.qc.ca/protection-renseignements-personnels/information-entreprises-privees/champ-application-loi_entreprises#:~:text=Que%20consid%C3%A8re%2Dt,de%20ces%20obligations.