POLITIQUE DE CONFIDENTIALITÉ ET DE PROTECTION DE LA VIE PRIVÉE

CALACS
CHÂTEAUGUAY
Centre d'Aide et de Lutte contre les Agressions à Caractère Sexuel

CALACS CHÂTEAUGUAY

MARS 2025

TABLE DES MATIÈRES

1. GÉNÉRALITÉS

1.1. PRÉAMBULE

Ce présent document aborde la gestion et la protection des renseignements confidentiels au sein du CALACS Châteauguay, et ce, en balisant le recueil, l'utilisation ainsi que la divulgation des informations personnelles à des fins justifiables liées aux ressources, au suivi des activités, telles que l'intervention, l'accompagnement et le soutien des personnes ainsi que la mobilisation des membres (bénévoles).

Il s'inscrit dans la mise en place de la réforme, depuis septembre 2022, de la Loi modernisant des dispositions législatives en matière de protection des renseignements personnels dans le secteur privé, aussi appelée Loi 25. Cette réforme modernise les règles protégeant les renseignements personnels au Québec afin qu'elles soient mieux adaptées aux nouveaux défis posés par l'environnement numérique et technologique actuel.

La présente Politique traite notamment les renseignements des utilisatrices, des membres (bénévoles), de la Collective (collective administrative) et de l'équipe de travail, afin de prévenir la divulgation inadéquate ou non essentielle des renseignements privés de ceux-ci.

De saines pratiques organisationnelles en matière de protection de la vie privée sont essentielles à la bonne gouvernance, à la responsabilisation envers ses membres et à la gestion du risque.

1.2. OBJECTIFS

- Le respect de la vie privée des personnes ci-haut mentionnées et la sécurité de leurs informations privées détenues physiquement et/ou électroniquement par le CALACS Châteauguay;
- Le développement et la supervision du mécanisme de gestion de l'utilisation de l'information, lors d'échanges internes et externes;
- L'obtention du consentement des particuliers en ce qui a trait au recueil, à l'utilisation et à la divulgation de leurs renseignements personnels;
- L'utilisation de l'information uniquement aux fins prévues;
- La vérification de l'exactitude de l'information et de sa conservation à des fins raisonnables;
- L'accès des particuliers à l'information recueillie à leur sujet;
- La protection de l'information contre tout accès, utilisation ou divulgation inappropriée.

1.3. ÉTENDUE

Cette politique s'applique à toutes les utilisatrices des services, les membres du CALACS, notamment les administratrices (Collective) et l'équipe de travail.

1.4. DÉFINITIONS

1.4.1. DÉSIGNATIONS

Les utilisatrices des services font référence aux personnes qui bénéficient de tous types de services d'aide du CALACS ayant communiqué leurs données en vue d'obtenir les dits services.

Les membres (bénévoles) font référence aux membres de l'organisme indépendamment de leurs statuts (militantes, solidaires, sympathisants) et les membres de la Collective adminis-trative (C.A).

Les donateurs font référence aux personnes ayant communiqué leurs données en vue de rester à l'affût de la programmation de l'organisme.

L'équipe de travail fait référence aux employées actives et inactives de l'organisme et aux stagiaires ayant communiqué leurs données en vue d'exercer leur emploi ou stage au CALACS.

1.4.2. RENSEIGNEMENT PERSONNEL

Toute information permettant d'identifier une personne, par exemple un numéro de téléphone, adresse, nom, dossier psycho-médical, notes évolutives, photo, et autre.

1.4.3. CONSENTEMENT

Lorsque l'on recueille des renseignements personnels auprès des différentes personnes désignées, il est primordial d'expliquer le but de cette collecte d'information et d'obtenir leur permission préalable. * Se référer à l'annexe 5 ci-bas pour obtenir le descriptif détaillé des renseignements demandés.

2. NORMES

Les informations personnelles des personnes désignées peuvent être utilisées aux fins de financement et programmes, de prestation des services d'aide, d'éducation et de sensibilisation du public et pour établir, maintenir et gérer les relations avec ces individus et organismes partenaires.

2.1. RESPONSABILITÉ

L'organisme est responsable de l'utilisation des informations qui lui sont transmises et s'engage à les protéger rigoureusement. L'équipe de travail et de militantes (bénévoles) disposant d'informations sensibles ont l'obligation de réserve et de confidentialité, en conformité avec la présente politique et l'esprit de la Loi; tout manquement à son respect pourra mener à des mesures disciplinaires pouvant aller jusqu'au congédiement des employées, stagiaires et à la terminaison de l'engagement bénévole, dans les cas jugés plus graves.

Toute question relatant la protection de la vie privée est intégrée aux programmes d'orientation et de formation des nouvelles employées et bénévoles.

L'organisme et toutes les personnes désignées dans cette Politique partagent la responsabilité de signaler tout incident de bris de confidentialité et de faire part de toutes préoccupations ou manquements eu égard à la présente Politique.

2.2. COLLECTE DES RENSEIGNEMENTS

L'organisme s'engage à agir en toute transparence dans la gestion des renseignements personnels en informant les personnes désignées de sa politique, ainsi qu'en veillant à leur accord par l'entremise de la signature d'un formulaire de consentement et en s'engageant à intervenir en cas d'incident.

La gestion adéquate de ces informations soutient la prise de décisions de la gouvernance et protège les droits de l'organisme et des personnes désignées. Ces informations permettent de préserver une preuve d'historique des individus et constituent une source d'information à leur sujet.

2.3. CONSENTEMENT

Les personnes désignées sont informées verbalement ou par écrit de toute collecte, utilisation ou communication de renseignements personnels et choisissent ou non de nous les divulguer.

2.4. UTILISATION ET COMMUNICATION

À moins d'avis contraire émis par la personne désignée ou par la loi applicable, les renseignements personnels ne seront jamais utilisés ou partagés dans des buts autres que ceux précisés lors de leur collecte.

Le CALACS Châteauguay s'engage à ne recueillir que les informations essentielles aux activités auxquelles les personnes désignées souhaitent participer et à utiliser un système de protection des données confidentielles.

Pour ce qui est du site internet de l'organisme, il est important de se référer à la Politique en vigueur à cet effet ou se référer à l'annexe du présent document.

2.5. CONSERVATION

L'organisme conservera les données des personnes désignées aussi longtemps que nécessaire afin d'assurer un bon déroulement des activités.

Pour les utilisatrices des services la durée de conservation des notes manuscrites au dossier est de 30 jours suivant la fin des services. Les données personnelles et les données statistiques seront supprimées définitivement seulement à la fin de l'année d'activité de chaque année se terminant le 30 juin.

Pour les membres (bénévoles) (militantes, solidaires, sympathisants) incluant les membres de la Collective administrative, la durée de conservation des informations est permanente ou jusqu'à la résiliation de l'adhésion du dit membre à l'organisme.

Pour les donateurs, la durée de conservation des informations est de 7 ans (suivant le calendrier de conservation en vigueur des dossiers).

Pour l'équipe de travail i.e. ses employées actives et inactives ainsi que les stagiaires, la durée de conservation des informations est de 7 ans pour tout dossier inactif.

Une fois cette durée écoulée, toute donnée relative dudit fichier sera effacée du système informatique et tout document papier sera déchiqueté sous la responsabilité d'un membre de l'équipe de travail ou de la Collective administrative.

2.6. MESURES PRÉVENTIVES

Le CALACS Châteauguay s'engage à restreindre l'accès aux dossiers des personnes désignées autant que possible en veillant à :

- Respecter les lieux de travail entre collègues;
- Maintenir et garder à jour un système informatique sécurisé répondant aux normes de l'industrie (cyber protection);
- Sécuriser les informations/les dossiers dans les bureaux et les filières de l'organisme;
- S'assurer que les bureaux des travailleuses soient exempts de données personnelles visibles ou accessibles (ex. : post-it avec informations).

2.7. TRANSPARENCE QUANT À L'ACCÈS AUX DONNÉES PERSONNELLES

Toutes les personnes désignées du CALACS Châteauguay seront en mesure de demander à consulter ou modifier ses propres renseignements personnels.

Toutes les personnes désignées seront également en mesure de se prévaloir du droit à l'oubli afin que ses données personnelles soient détruites de manière définitive de nos systèmes et dossiers.

À tout moment, les personnes désignées peuvent refuser, ou retirer leur consentement à certains, ou tous les buts mentionnés lors de leur inscription en communiquant avec l'organisme.

2.8. PROCESSUS DE PLAINTE

Toute plainte doit être transmise à chantal.robitaille@calacs-chateauguay.ca ou au 450 699-8258, poste 203, selon les procédures en vigueur. La plainte sera traitée selon les politiques en vigueur.

3. RESPONSABILITÉS

3.1. LA COLLECTIVE ADMINISTRATIVE (C.A.)

La Collective administrative :

- Approuve ce présent document et ses futures modifications;
- S'assure que la travailleuse responsable effectue un suivi rigoureux.

3.2. LA COORDONNATRICE

La coordonnatrice:

- Maintient les employées et les militantes (bénévoles) à jour quant aux enjeux de la confidentialité des données sensibles;
- Assure la mise en place de bonnes pratiques lors de l'utilisation de renseignements personnels;
- Recommande des modifications de la Politique à la Collective administrative, le cas échéant.

4. TABLEAU DES MODIFICATIONS ++ de modifications

ENTRÉE EN VIGUEUR	ATTENDUES	RÉSULTATS
2022-09-22	Désignation d'une personne responsable de la protection des renseignements personnels (PRP) et identification sur le web Élaboration d'un registre des incidents de confidentialité Signalement des incidents comportant un risque de préjudice grave à la Commission d'accès à l'information (CAI)	Choix de la personne désignée Formulaire de désignation signé. Registre en vigueur Signalements effectués
2023-09-22	Élaboration d'une Politique et des pratiques encadrant la gouvernance des RP et publication sur le site web Transfert de données à un tiers doit faire l'objet d'une entente préalable Transfert à l'extérieur du Qc doit faire l'objet d'une évaluation et d'une entente Obtention du consentement manifeste des personnes et les informations sur la Loi Élaboration d'une politique de conservation et de destruction des RP	Politique adoptée. Ententes de confidentialité signées. Formulaire d'adhésion des membres modifié.
2024-09-22	Droit à la portablité – communicabilité des informations (RP) dans un format technologique structuré (et couramment utilisé à la victime et aux instances gouvernementales). Développer ou consolider une infra-structure technologique de stockage, d'encryptage et de gestion des RP.	Avoir informé l'équipe responsable de l'entretien, la mise à jour ou du développement de nos systèmes informatiques de nos nouveaux besoins en lien avec la portabilité des renseignements per-sonnels

5. ANNEXE I – RENSEIGNEMENTS RECENSÉS

Voici une énumération non exhaustive des renseignements personnels qui peuvent être demandés :

Tronc commun pour les membres (incluant les personnes utilisatrices des services) :

- Nom, prénom
- Âge
- Genre
- Adresse de résidence
- Numéro de téléphone
- Adresse courriel

Employées :

- Nom et prénom
- Date de naissance (avec année)
- Numéro d'assurance sociale
- Adresse courriel
- Adresse postale
- Numéro de téléphone
- Coordonnées bancaires
- Pièces d'identité
- Situation familiale
- Renseignements médicaux
- Date d'entrée en fonction
- Vérification des antécédents judiciaires

Collective administrative :

- Nom et prénom
- Date de naissance (avec année)
- Adresse courriel
- Adresse postale
- Numéro de téléphone
- Pièces d'identité avec photo
- Date début de mandat
- Vérifications des antécédents judiciaires

Les documents papier utilisés à des fins de collecte d'information seront détruits dès que les renseignements personnels se retrouveront dans le logiciel de collecte de données et autres fournisseurs s'il y a lieu. Le CALACS s'engage à conserver ces documents sous clé jusqu'à la destruction de ceux-ci.

6. ANNEXE II – ACCÈS AUX RENSEIGNEMENTS PERSONNELS INFORMATIQUES

- ASO Logiciel de gestion des données des membres, participantes, bénévoles et partenaires :

  - Accès complet au logiciel par le personnel en lien avec la gestion des données, à la suite d'une formation de base et restreint par un mot de passe;
  - Accès aux stagiaires sous supervision d'une employée et restreint par un mot de passe personnalisé et temporaire, pour la durée des fonctions.

- Dossiers et fichiers des utilisatrices, membres (bénévoles) et partenaires :

  - Pour les utilisatrices, accès complet du personnel dans le logiciel ASO.
  - Pour les membres, accès complet du personnel, restreint par un mot de passe pour l'accès aux fichiers.
  - Pour les partenaires, accès complet en fonction des dossiers des travailleuses.

- Dossiers des employées sur le serveur :

  - Accès complet du personnel dans la base de données[1] ou en filière.

- Dossier de gestion de la paie, des assurances collectives et régime de retraite :

  - Plateforme des paies accessible par mot de passe personnalisé par l'employée à la comptabilité;
  - Données pertinentes transmises de façon papier à la responsable de la comptabilité.
  - Base de données, filière et fournisseurs.

[1] Référence au DATA

7. ANNEXE III – GESTION DES INCIDENTS

Incidents de confidentialité

Exemples des incidents possibles :

- Altération délibérée
- Communication accidentelle
- Communication délibérée
- Consultation non autorisée
- Cyberattaque (virus, logiciel espion, etc.)
- Défaillance technique
- Destruction accidentelle ou délibérée
- Divulgation accidentelle ou délibérée
- Erreur humaine
- Hameçonnage (phishing)
- Ingénierie sociale[i]
- Perte d'accès aux renseignements
- Utilisation incompatible
- Vol de renseignements, rançongiciel
- Autre

Obligations de l'organisation en cas d'incident

Inscrire l'incident dans le registre des incidents de confidentialité des renseignements personnels. Évaluer si l'incident de confidentialité pourrait causer un préjudice sérieux [ii]aux personnes concernées.

Signaler tout incident dans les meilleurs délais possibles, sur nos réseaux sociaux en fonction des paramètres existants.

Prendre des mesures pour diminuer les risques de préjudice et éviter que des incidents similaires ne se produisent à l'avenir.

Aviser toute personne dont les renseignements personnels ont été compromis si l'incident présente un risque sérieux de préjudice.

Aviser la Commission d'accès à l'information du Québec d'un incident de confidentialité impliquant un renseignement personnel si l'incident présente un risque sérieux de préjudice.

Fournir à la Commission d'accès à l'information du Québec toute information supplémentaire connue après l'envoi de l'avis initial.

Pour plus d'informations sur les obligations en cas d'incident de confidentialité, consulter le site Web de la Commission d'accès à l'information du Québec à l'adresse suivante: https://www.cai.gouv.qc.ca/incident-de-confidentialite-impliquant-des-renseignements-personne ls/

Plan de gestion des incidents

Réception de la plainte : Une personne envoie une plainte à l'organisation concernant la manière dont ses renseignements personnels ont été traités ou demande une désindexation.

Enregistrement de la plainte : L'organisation enregistre la plainte dans un système de suivi des plaintes. Cela peut être un outil numérique ou un registre manuel, selon la taille et les ressources de l'organisation.

Évaluation de la plainte : Un responsable ou un comité désigné examine la plainte pour déterminer si elle est valide et si elle relève de la Loi 25. Il est essentiel d'évaluer si les droits de la personne, en vertu de la loi, ont été violés.

Enquête : Si la plainte est jugée valide, une enquête plus approfondie est menée pour comprendre les circonstances de l'incident. Cela peut impliquer de consulter des dossiers, de parler à des membres du personnel ou d'examiner des procédures internes.

Résolution : Sur la base des résultats de l'investigation, l'organisation prend des mesures pour résoudre la plainte. Cela peut impliquer des modifications des procédures, une formation du personnel, ou, dans le cas d'une demande de désindexation, la suppression de certaines informations des résultats de recherche.

[i] L'ingénierie sociale est une technique de manipulation utilisée pour inciter une personne à transmettre elle-même des données sensibles. Ces données peuvent être des renseignements personnels ou des informations confidentielles permettant d'accéder au réseau informatique d'une organisation. Une fois infiltré dans un système, le cyberfraudeur peut subtiliser les données auxquelles il a accès pour ensuite les vendre ou les utiliser à des fins malveillantes. (Définition tirée de : https://www.ulaval.ca/cybersecurite/ingenierie-sociale)

[ii] Pour tout incident de confidentialité, l'entreprise doit évaluer la gravité du risque de préjudice pour les personnes concernées. Pour ce faire, elle doit considérer, notamment : La sensibilité des renseignements concernés; Les conséquences appréhendées de leur utilisation; La probabilité qu'ils soient utilisés à des fins préjudiciables.(Tiré du site web de la Commission d'accès à l'information : https://www.cai.gouv.qc.ca/protection-renseignements-personnels/information-entreprises-privees/incidents-confidentialite-mesures-securite-entreprises#:~:text=Pour%20ce%20faire%2C%20elle%20doit,utilis%C3%A9s%20%C3%A0%20des%20fins%20pr%C3%A9judiciables.).