

**POLITIQUE DE PROTECTION DES RENSEIGNEMENTS PERSONNELS ET
CONSENTEMENTS DU SYNDICAT DES COPROPRIÉTAIRES D'ÉMERAUDE DES RIVES- PHASE 1**

La présente Politique de protection des renseignements personnels établit les pratiques du Syndicat des copropriétaires

Cette Politique vise à vous informer sur la collecte, l'utilisation ou la divulgation de vos renseignements personnels à titre de copropriétaires de l'Immeuble, à établir de bonnes pratiques en la matière, ainsi qu'à recueillir les consentements nécessaires aux fins du bon fonctionnement du syndicat.

Est un renseignement personnel, tout renseignement qui concerne une personne physique et permet de l'identifier.

1. Responsable de la protection des renseignements personnels

Le conseil d'administration veille à assurer le respect et la mise en œuvre de la *Loi sur la protection des renseignements personnels dans le secteur privé en désignant une personne Responsable*.

Le conseil d'administration désigne cette personne parmi ses membres.

2. Source de collecte des renseignements personnels

A) Création du fichier

Le Syndicat peut recueillir des informations personnelles sur tout copropriétaire, locataire et/ou occupant de l'immeuble à des fins légitimes en relation avec ses devoirs d'administration de l'immeuble.

À cet effet, le Syndicat est susceptible de recueillir des informations personnelles avant même la signature de tout acte de vente et/ou de tout bail ou autre document contractuel, aux fins d'obtenir les renseignements sur les occupants, dont notamment mais sans limiter la généralité de ce qui précède, afin d'obtenir leurs coordonnées et de communiquer avec eux;

Le Syndicat confie au conseil d'administration et/ou au gestionnaire, la collecte, la gestion et la mise à jour des coordonnées de ce fichier dans le cadre de ses activités.

La banque de données est complétée des informations qui y sont reliées.

B) Autres sources de collecte des renseignements personnels

Le Syndicat recueille des renseignements personnels concernant les copropriétaires, locataires, occupants, visiteurs, dont lorsqu'ils communiquent avec lui de diverses façons, notamment :

- lors de toute communication écrite, téléphonique ou électronique avec copropriétaire (ou locataire, ou occupant) avec le Syndicat;
- lors de la tenue des assemblées;
- lors du paiement des charges communes;
- à tout autre moment aux fins de la réalisation de la mission du Syndicat aux termes de la Loi et de la déclaration de copropriété;

Le Syndicat recueille également des renseignements personnels concernant les différentes personnes précédemment identifiées, lorsque, notamment :

- ils entrent dans l'Immeuble grâce à leurs puces électroniques;
- ils sont captés par l'une des caméras de surveillance se trouvant dans l'Immeuble, dans les parties communes ou les parties communes à usage restreint, le cas échéant.

Il revient à chaque copropriétaire d'informer son locataire et/ou occupant qu'en acceptant d'occuper une partie privative au sein de l'immeuble administré par le Syndicat, il consent implicitement au recueil de ses renseignements personnels, à moins d'indication contraire.

Le Syndicat recueille également des renseignements d'autres partenaires avec lequel il doit transiger, notamment les fournisseurs de service.

3. Nature des renseignements personnels colligés

Le Syndicat recueille dans le cadre de ses activités, les renseignements personnels suivants:

- Les coordonnées de base que sont :
 - le nom des copropriétaires;
 - Le numéro d'appartement, et des stationnements et casiers éventuels.
 - les numéros de téléphone;
 - les adresses courriel;
 - les contacts en cas d'urgence;
 - les coordonnées bancaires;
 - le modèle et la description du véhicule;
 - le nom des occupants, locataires et visiteurs des unités et le lien entre le copropriétaire, les locataires, les occupants et les visiteurs;
 - tous autres renseignements pouvant s'avérer utiles aux fins de la réalisation de la mission du Syndicat, aux termes de la Loi et de la déclaration de copropriété;
- Ainsi que :
 - la présence aux assemblées, leurs enregistrements vidéo, ainsi que le registre des votes et des procurations;
 - tous autres renseignements pouvant s'avérer utiles aux fins de la réalisation de la mission du Syndicat, aux termes de la Loi et de la déclaration de copropriété;

4. Utilisation des renseignements personnels par le Syndicat

De façon générale, le conseil d'administration utilise les renseignements personnels pour:

- Appliquer la déclaration de copropriété et s'assurer de son respect;
- Assurer le paiement des charges communes;
- Répondre à une demande d'information;
- Informer des modifications apportées à la déclaration de copropriété, aux règlements de la copropriété, et/ou pour d'autres objectifs administratifs;

5. Communication des renseignements personnels

Les administrateurs peuvent communiquer les renseignements personnels auprès du gestionnaire de l'immeuble et du personnel de la compagnie de gestion, s'il y a lieu. Le conseil d'administration pourra aussi communiquer les renseignements personnels à tous autres tiers, notamment à toute plateforme électronique de gestion, à tous prestataires et professionnels, dans la mesure où le partage de ces renseignements s'avère utile aux fins de la réalisation de la mission du Syndicat, aux termes de la Loi et de la déclaration de copropriété.

Au moment de partager des renseignements, le Syndicat s'informe auprès des tiers quant à la nature des renseignements recueillis et vérifie que ces renseignements ne soient pas transmis à d'autres tiers et/ou partenaires commerciaux.

6. Aucune autre communication des renseignements à des fins de prospection commerciale

Sauf pour les fins de communication précitées, le Syndicat a comme politique de ne pas divulguer ni vendre à des tiers, aucun renseignement personnel sur les copropriétaires pour des fins de prospection commerciale ou philanthropique.

7. Communication nécessaire pour se conformer à la loi

Le Syndicat se réserve le droit de divulguer certains renseignements personnels concernant les copropriétaires, locataires, occupants et visiteurs s'il estime que cela est nécessaire compte tenu de ses obligations au terme de la déclaration de copropriété et de la Loi. Ainsi, le Syndicat peut partager des informations dans le cadre de procédures, pour répondre à une ordonnance de la Cour ou à l'envoi d'un subpoena. Le Syndicat peut également communiquer des renseignements personnels si une agence gouvernementale ou un organisme d'enquête public l'exige.

8. Accès limité aux renseignements personnels

À l'interne, le Syndicat ne permet qu'un accès limité aux renseignements personnels. Les administrateurs et/ou le gestionnaire dont le mandat est échu doivent purger leurs systèmes de tous renseignements personnels obtenus dans le cadre de leur mandat, après s'être assurés

d'avoir transféré l'ensemble des informations, dossiers, et/ou renseignements, auprès de la nouvelle administration et/ou du nouveau gestionnaire. L'ancien administrateur et/ou gestionnaire ne saurait notamment utiliser les adresses courriels des copropriétaires, qu'il a obtenues dans le cadre de son mandat, à des fins personnelles.

9. Stockage et sécurité

Tous les renseignements personnels fournis au Syndicat sont conservés sur des serveurs sécurisés, à accès restreint du conseil d'administration et/ou des employés de la compagnie de gestion.

Le Syndicat utilise les moyens techniques raisonnables pour assurer un environnement sécuritaire et protéger les renseignements personnels, tels que : barrières coupe-feu, usage d'antivirus, gestion des accès, détection des intrusions, copie de sauvegarde régulière. Cependant, étant donné la nature même du réseau public qu'est l'internet, les copropriétaires reconnaissent et acceptent que la sécurité des transmissions via internet ne puisse être garantie. En conséquence, le Syndicat en peut garantir ni n'assume aucune responsabilité pour toute violation de confidentialité, piratage, virus, perte ou altération des données transmises par Internet.

10. Conservation

Le Syndicat utilise et conserve les renseignements personnels pour la durée nécessaire à l'objet de la collecte des renseignements.

Toutefois, le Syndicat se réserve le droit de détenir, pour une durée raisonnable, certains renseignements personnels pour être en règle avec la Loi, prévenir la fraude, collecter des frais dus, résoudre une réclamation ou certains autres problèmes s'y rattachant, coopérer à une enquête et pour tout autre acte permis par la loi.

À l'expiration de ce délai, les renseignements personnels seront délestés des serveurs du Syndicat.

11. Incidents de confidentialité

Un incident de confidentialité correspond à un 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.

Le responsable de la protection des renseignements personnels, s'il a des motifs de croire que s'est produit un incident de confidentialité impliquant un renseignement personnel qu'il détient, doit prendre les mesures raisonnables pour diminuer les risques qu'un préjudice soit causé et éviter que de nouveaux incidents de même nature ne se produisent.

Le responsable de la protection des renseignements personnels procède à l'évaluation du préjudice selon la procédure prévue à l'Annexe 1.

Le responsable de la protection des renseignements personnels tient un registre des incidents de confidentialité (Annexe 2) et, sur demande de la Commission d'accès à l'information, lui en transmet une copie.

Les renseignements contenus au registre des incidents de confidentialité doivent être tenus à jour et conservés pendant une période minimale de cinq ans après la date ou la période au cours de laquelle le responsable a pris connaissance de l'incident.

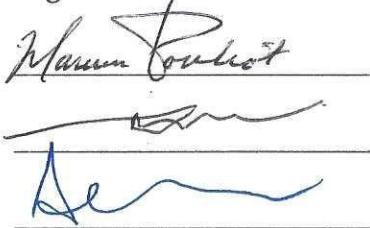
12. Lois applicables et juridiction

La présente Politique de protection des renseignements personnels est régie par les lois de la province de Québec et les lois du Canada qui s'y appliquent.

Nom des responsables de la protection des renseignements personnels :

Maurice Pouliot et Francine Faille

Signature des membres du conseil d'administration:



Two handwritten signatures are shown. The top signature is "Maurice Pouliot" in blue ink. The bottom signature is "Faille" in blue ink, with a small "M" written above it. Both signatures are placed over two horizontal lines.

Date : 7 août 2023

ANNEXE 1 : Procédure à suivre en cas d'incident de confidentialité

Les étapes qui suivent peuvent être réalisées simultanément.

1. **Évaluer la situation.** Le responsable qui a des raisons de croire que s'est produit un incident de confidentialité impliquant un renseignement personnel qu'il détient doit notamment :
 - a. Établir les circonstances de l'incident;
 - b. Identifier les renseignements personnels impliqués;
 - c. Identifier les personnes concernées;
 - d. Trouver le problème, que ce soit une erreur, une vulnérabilité, etc. Cette évaluation doit se poursuivre tant que tous les éléments n'ont pas été identifiés.
2. **Diminuer les risques.** Le responsable doit prendre rapidement les mesures raisonnables qui s'imposent afin de diminuer les risques qu'un préjudice, qu'il soit sérieux ou non, ne soit causé et pour éviter que de nouveaux incidents de même nature ne surviennent, par exemple :
 - a. Cesser la pratique non autorisée;
 - b. Récupérer ou exiger la destruction des renseignements personnels impliqués;
 - c. Corriger les lacunes informatiques.
3. **Identifier la nature du préjudice.** L'objectif consiste à déterminer s'il faut aviser la CAI et les personnes concernées ainsi qu'établir les mesures à mettre en place pour diminuer les risques notamment :
 - a. Incrire une note dans les dossiers visés par un risque de vol d'identité;
 - b. Exiger des vérifications supplémentaires.

Évaluation du préjudice

Lors d'un incident de confidentialité, le responsable doit évaluer s'il en découle un risque qu'un préjudice soit causé à une personne dont un renseignement personnel est concerné. Il doit alors considérer plusieurs facteurs, dont :

- La sensibilité des renseignements personnels tels un renseignement financier ou un renseignement d'identité;
- Les conséquences appréhendées de l'utilisation de ces renseignements comme :
 - o Un vol d'identité;
 - o Une fraude financière;
 - o Une atteinte importante à la vie privée.
- La probabilité que ces renseignements puissent être utilisés à des fins préjudiciables.

Un préjudice sérieux correspond à un acte ou à un événement susceptible de porter atteinte à la personne concernée ou à ses biens et de nuire à ses intérêts de manière non négligeable. Il peut conduire, par exemple :

- À l'humiliation;
- À une atteinte à la réputation;
- À une perte financière;

- À un vol d'identité;
- À des conséquences négatives sur un dossier de crédit;
- À une perte d'emploi.

4. Incrire l'incident au registre, que le risque de préjudice soit qualifié ou non de sérieux.

5. S'il y a un risque de préjudice sérieux. Le responsable doit :

- Aviser la commission d'accès à l'information dès que possible, même s'il n'a pas colligé l'ensemble des informations relatives à l'incident, et remplir la déclaration par la suite. Il peut ainsi aviser la commission d'accès à l'information de l'incident et, plus tard, confirmer le nombre de personnes concernées.

- Aviser toute personne dont un renseignement personnel est concerné par l'incident, à moins que cet avis ne soit susceptible d'entraver une enquête. Un délai peut s'appliquer entre le moment où le responsable prend connaissance de l'incident et celui où il en avise les personnes concernées. Ce délai peut être nécessaire afin, par exemple, d'identifier les renseignements personnels impliqués, les personnes concernées, la faille de sécurité et pour colmater celle-ci ou pour éviter d'entraver une enquête en cours.

Ces avis sont obligatoires.

6. S'il y a un risque de préjudice sérieux : le responsable peut aussi aviser toute personne ou tout organisme susceptible de diminuer ce risque. À cette fin, il ne peut lui communiquer que les renseignements personnels qui sont nécessaires à la poursuite de cet objectif. L'obtention du consentement de la personne concernée par les renseignements transmis n'est pas requise. Toutefois, la personne responsable de la protection des renseignements personnels doit enregistrer la communication pour garder des traces documentaires de celle-ci comme :

- À qui ces renseignements sont communiqués;
- Dans quelles circonstances;
- Quels renseignements ont été transmis;
- Quels sont les objectifs de cette démarche.

ANNEXE 2 : Registre des incidents de confidentialité