

## **POLITIQUE CONCERNANT LA PROTECTION DES RENSEIGNEMENTS PERSONNELS**

### **HOGUE, FORTIER, FRÉCHETTE INC. (ci-après appelée « l'Organisation »)**

Le droit au respect de sa vie privée est un principe reconnu pour tous. Dans bien des situations, des personnes fournissent leurs renseignements personnels afin d'obtenir certains services ou produits et ce, auprès de beaucoup d'organisations et même auprès d'organismes publics.

Il est donc important, et même primordial, de bien protéger ces renseignements personnels afin d'éviter des désagréments considérables et surtout inutiles aux individus.

Au Québec, les dispositions de la *Loi sur la protection des renseignements personnels dans le secteur privé*, RLRQ, c. P-39.1 ont traité l'aspect de la protection des renseignements personnels appartenant à toute personne. Mais une modification a été apportée à ladite loi par la nouvelle *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*, communément appelée la Loi 25, qui a été adoptée le 21 septembre 2021 et sanctionnée le 22 septembre 2021 (ces deux lois précitées, ainsi que toute loi pouvant les remplacer de temps à autre, étant ci-après collectivement appelées la « **Législation québécoise** »).

Dans le cadre de ses activités, l'Organisation reconnaît qu'elle recueille et détient les renseignements personnels d'autrui. Et par conséquent, elle est tenue de se conformer à la Législation québécoise.

Par ailleurs, les membres professionnels de l'Organisation ainsi que leur collaborateurs sont toujours soumis aux règles de la protection de la confidentialité et de la protection du secret professionnel propres à la profession notariale.

#### **Le but de cette politique - les mesures**

Cette politique de l'Organisation vise à informer son personnel des mesures décrites aux présentes qui sont en lien avec la Législation québécoise et qui sont appropriées pour protéger les renseignements personnels :

1. Les mesures requises pour se conformer à la Législation québécoise
2. Les mesures pour son système informatique
3. Les mesures pour l'inventaire des renseignements personnels
4. Les mesures pour son personnel
5. Les mesures pour son site web
6. Les mesures pour la voûte matérielle

Cette politique de l'Organisation traite de ces mesures mentionnées ci-dessus de manière ci-après décrite et ce, pour le bénéfice des membres de son personnel auxquels cette politique s'adresse notamment :

- Les mesures déjà mises en oeuvre par l'Organisation
- Les mesures que l'Organisation verra à mettre en oeuvre dans les meilleurs délais
- Les mesures que l'Organisation n'entend pas mettre en oeuvre

### **Sessions pour informer le personnel de l'Organisation**

L'Organisation prévoit donner aux membres de son personnel qui traitent ou travaillent avec des renseignements personnels dans le cadre de leurs fonctions, des sessions de formation et/ou d'information concernant les renseignements personnels et leur protection ainsi que la confidentialité requise pour de tels renseignements.

L'Organisation pourra modifier, à sa discrétion et de temps en temps, cette politique et dans un tel cas, elle en avisera tous les membres de son personnel en leur remettant ou leur donnant accès à la politique ainsi modifiée.

Le personnel de l'Organisation devra en tout temps respecter cette politique afin de protéger au mieux les renseignements personnels de ses clients. De plus, tous les membres de son personnel devront se conformer aux mesures mises en oeuvre par l'Organisation en lien avec la présente politique.

L'Organisation verra à remettre ou rendre accessible une copie de cette politique à chacun des membres de son personnel, tant actuels que futurs, peu importe que ceux-ci soient des employés ou des pigistes, y compris les membres de son personnel agissant à titre de dirigeants de l'Organisation.

### **Interprétation**

Il est entendu qu'aux fins de cette politique, l'expression « **Organisation** » sera utilisée pour désigner un bureau de professionnels.

En effet, toute personne physique ou morale qui possède, exploite ou constitue un bureau de professionnels assujettis au *Code des professions* et offrant des services à la population constitue une « **entreprise** » au sens de la Législation québécoise et par conséquent, doit se conformer à ses dispositions.

L'expression « **clients** » désignera à la fois les clients et les utilisateurs d'une Organisation.

## **PARTIE 1**

### **LA LÉGISLATION QUÉBÉCOISE ET SES IMPLICATIONS POUR L'ORGANISATION**

#### **Principe général concernant la vie privée**

Chacun a droit au respect de sa vie privée, incluant ses renseignements personnels, sauf son consentement en cas d'atteinte à sa vie privée.

## **But de la Législation québécoise**

La Législation québécoise vise à assurer la protection et la confidentialité des renseignements personnels et de la vie privée des personnes physiques faisant affaire avec ce qu'on appelle une « **entreprise** » qui est assujettie à la Législation québécoise.

## **Exploiter une « entreprise » au sens de la Législation québécoise**

Toute entreprise qui recueille, détient, communique et/ou utilise des renseignements personnels dans le cadre de ses activités, que ces dernières soient commerciales ou non, est assujettie à la Législation québécoise car elle exploite alors une « **entreprise** » au sens de la Législation québécoise et par conséquent, elle doit en respecter les dispositions.

## **Deux grands principes établis par la Législation québécoise**

La Législation québécoise a mis de l'avant les deux principes suivants : 1) une entreprise ne peut recueillir que les renseignements personnels nécessaires aux fins déterminées pour leur collecte et ne peut utiliser ces renseignements qu'aux fins pour lesquelles ils ont été recueillis, sauf s'il y a consentement de la personne concernée; et 2) personne ne peut communiquer à un tiers les renseignements personnels qu'il détient sur autrui, à moins que la personne concernée n'y consente ou que la Législation québécoise ne le prévoit ou ne l'exige.

## **Ce qui constitue un renseignement personnel - Exemples**

C'est la définition d'un renseignement personnel, telle qu'elle est établie par la Législation québécoise, qui détermine si les informations recueillies et détenues par une entreprise constituent ou non ce qu'on appelle un « renseignement personnel » au sens de la Législation québécoise. En effet, si une entreprise ne recueille aucun renseignement personnel auprès de ses clients, elle n'est pas alors tenue de respecter les dispositions de la Législation québécoise.

Selon la Législation québécoise, tout renseignement qui concerne une personne physique et qui permet d'identifier celle-ci, est considéré comme étant un renseignement personnel peu importe la nature du support et la forme sous laquelle ce renseignement est rendu accessible, soit écrite, graphique, sonore, visuelle, informatisée ou autre.

Un renseignement personnel, c'est donc toute information reliée ou concernant une personne physique en particulier qui permet de l'identifier ou qui peut être utilisée pour l'identifier d'une manière spécifique, que ce soit en utilisant cette information seulement ou encore, cette information couplée avec d'autres renseignements détenus par une entreprise, y compris les informations fournies à l'entreprise par les clients eux-mêmes; c'est pourquoi on parle parfois de renseignements personnellement identifiables.

Ne sont pas considérés comme constituant des renseignements personnels toutes les informations ou renseignements devenus ou rendus anonymes ou dépersonnalisés ou qui ont été agrégés de manière à ne pouvoir identifier spécifiquement et de quelque manière que ce soit une personne physique.

Par exemple, si une entreprise offre aux personnes accédant à son site web de s'abonner à ses infolettres, alors cette entreprise recueille et détient des renseignements personnels sur les personnes

demandant cet abonnement, soit leurs nom, adresse civique, numéro de téléphone, adresse courriel, âge, etc. et ce, même s'il ne s'agit pas d'un site web transactionnel.

Par contre, le fait pour une personne de se connecter au site web d'une entreprise implique que cette dernière a accès à l'adresse IP de cette personne mais cet accès seul ne permet pas d'identifier cette personne en particulier, dans le sens que ce seul accès à l'adresse IP n'est pas considéré comme constituant une collecte de renseignements personnels.

### **En quoi consiste un renseignement personnel « sensible »?**

Un renseignement personnel est considéré comme sensible lorsque de « *par sa nature ou en raison du contexte de son utilisation ou de sa communication, il suscite un haut degré d'attente raisonnable en matière de vie privée* ». Cependant, il semble bien que cette notion ainsi présentée soit très subjective puisque la sensibilité d'un renseignement personnel dépend alors du contexte de son utilisation ou de sa communication.

Malgré cela, on peut constater que certaines catégories de renseignements personnels sont généralement considérées comme sensibles en raison des risques particuliers pour les personnes qui sont associés à la collecte, à l'utilisation ou à la communication de ces catégories de renseignements. En effet, certaines catégories de renseignements personnels sont souvent considérées comme sensibles et par conséquent, doivent faire l'objet d'une meilleure protection avec des mesures de sécurité adéquates et plus élevées.

Il s'agit notamment de renseignements portant sur la santé, les finances ou les revenus, la réputation des personnes, les origines ethniques et raciales, les opinions politiques, la vie sexuelle ou l'orientation sexuelle et les croyances religieuses ou philosophiques, ainsi que les données génétiques et biométriques.

Dans le cadre d'une évaluation pour savoir si des renseignements personnels sont considérés comme sensibles ou non, cela variera en fonction des faits de chaque cas. En fait, tout renseignement personnel peut devenir sensible selon le contexte s'appliquant à celui-ci.

Par exemple, des renseignements bien anodins lorsqu'ils sont pris isolément, comme le nom et une adresse de courriel, peuvent devenir sensibles lorsqu'ils sont associés à des services qui peuvent révéler les activités et les préférences personnelles des utilisateurs, c'est-à-dire si ces renseignements sont utilisés dans un autre contexte. Ainsi, le nom et l'adresse des abonnés d'une revue d'information ne sont généralement pas considérés comme des renseignements sensibles mais cependant, le nom et l'adresse des abonnés de certains périodiques spécialisés pourraient l'être.

Également, si des renseignements personnels sont combinés, ils pourraient possiblement être utilisés par des personnes malveillantes aux fins d'usurper les identités des personnes concernées, ce qui exige alors des mesures de sécurité plus élevées.

Par exemple, si la collecte, l'utilisation ou la communication non autorisée de renseignements personnels sensibles, comme le fait qu'une personne soit atteinte d'une infection transmissible sexuellement, pourrait entraîner une stigmatisation sociale, des problèmes émotifs et une atteinte à la réputation à long terme pour les personnes concernées, les renseignements doivent alors être protégés par des mesures de sécurité rigoureuses et élevées.

## Organisations et renseignements personnels

Il est reconnu que les bureaux de professionnels recueillent, détiennent et parfois communiquent des renseignements personnels appartenant à leurs clients, dans le but notamment de leur rendre les services que ceux-ci ont demandé.

La Législation québécoise s'applique aux renseignements personnels détenus par tout bureau de professionnels dont certains membres ou tous les membres font partie d'un ordre professionnel ou d'une association professionnelle, si cela est prévu par le *Code des professions* (RLRQ c. 26).

On pourrait vouloir prétendre que les professionnels, qui sont déjà soumis à leur code de déontologie ou au *Code des professions*, se trouveraient ainsi exemptés des dispositions de la Législation québécoise mais il ne pourra jamais en être de même concernant les autres membres du personnel des bureaux de professionnels puisque ceux-ci ne sont pas soumis à un code de déontologie ou au *Code des professions*.

C'est donc dire qu'un bureau de professionnels est visé par les dispositions de la Législation québécoise, et non pas seulement les professionnels exerçant dans ce bureau.

## Différentes obligations de l'Organisation selon la Législation québécoise - Exceptions

### Responsabilité pour la protection des renseignements

L'Organisation a la responsabilité de protéger les renseignements personnels de ses clients qu'elle recueille et détient. La plus haute autorité de l'Organisation doit assumer la fonction de responsable de la protection de ces renseignements personnels (ci-après appelé le « **Responsable** ») ou déléguer par écrit cette fonction à une autre personne au sein de l'Organisation. Le titre et les coordonnées de ce Responsable doivent être accessibles aux clients de l'Organisation.

En l'occurrence, le Responsable désigné par l'Organisation est :

M<sup>e</sup> Roxanne Duhaime, Notaire  
7160, boulevard Pie-IX, bureau 201  
Montréal (Québec) H2A 2G4  
(514) 727-9100  
[rduhaime@hffnotaires.ca](mailto:rduhaime@hffnotaires.ca)

### Politiques et pratiques pour encadrer la gouvernance des renseignements personnels

L'Organisation doit déterminer et implanter des politiques et des pratiques approuvées par le Responsable qui auront pour but d'encadrer sa gouvernance à l'égard des renseignements personnels de ses clients et qui permettront d'en assurer la protection et la confidentialité; de plus, l'Organisation doit rendre accessible l'information au sujet des politiques implantées. Ces politiques de l'Organisation doivent notamment prévoir l'encadrement s'appliquant à la conservation et à la destruction des renseignements personnels de ses clients, les rôles et les responsabilités des membres de son personnel tout au long du cycle de vie de ces renseignements et un processus pour traiter les plaintes en relation avec la protection des renseignements de ses clients.

### Obligations en lien avec la collecte de renseignements personnels

L'Organisation doit déterminer les fins pour lesquelles elle veut recueillir des renseignements personnels et ce, avant même de procéder à leur collecte, et elle doit aussi recueillir seulement les renseignements nécessaires aux fins ainsi déterminées.

L'Organisation doit notamment recueillir des renseignements personnels afin de procéder à la vérification de l'identité des parties à un acte notarié ou des intervenants nécessaires ou encore pour procéder à l'enregistrement de document sensible tel le testament ou le mandat de protection.

### Obligation d'information des personnes concernées

L'Organisation doit informer toute personne concernée par la collecte de ses renseignements, au moment de la collecte et par la suite, sur demande, des éléments suivants : 1) les fins pour lesquelles ses renseignements sont recueillis; 2) les moyens par lesquels ceux-ci sont recueillis; 3) ses droits d'accès et de rectification concernant ses renseignements; et 4) son droit de retirer son consentement à la communication ou à l'utilisation de ses renseignements recueillis.

Toute personne concernée a le droit d'être informée du nom du tiers pour qui la collecte de ses renseignements est faite, si tel est le cas, ainsi que du nom des tiers ou des catégories de tiers à qui il est nécessaire de communiquer ses renseignements personnels, si applicable.

### Obligation de divulguer tout incident de confidentialité - Tenue d'un registre

Advenant qu'un incident de confidentialité se produise et qu'il implique un renseignement personnel que l'Organisation détient, celle-ci 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. Dans le but d'évaluer qu'un incident de confidentialité survenu présente un tel risque, l'Organisation doit considérer la sensibilité de tel renseignement, les conséquences possibles suite à son utilisation et la probabilité qu'il soit utilisé à des fins préjudiciables ou malfaisantes.

L'Organisation doit tenir un registre des incidents de confidentialité et en transmettre sur demande une copie à la Commission d'accès à l'information du Québec (la « **Commission** »); ce registre doit être conservé pendant une période minimale de cinq ans suivant tout incident dont l'Organisation a pris connaissance. L'Organisation doit divulguer tout incident par un avis écrit envoyé à la Commission et à toute personne concernée. Un règlement a précisé le contenu de ces avis et du registre des incidents à tenir.

### Exceptions pour une utilisation à une autre fin, sans le consentement de la personne concernée

La Législation québécoise prévoit qu'un renseignement personnel ne peut être utilisé qu'aux fins pour lesquelles il a été recueilli, sauf en obtenant le consentement de la personne concernée, mais elle prévoit aussi deux exceptions à ce principe.

Ces deux exceptions s'appliquent à toutes les organisations visées par la Législation québécoise pour leur permettre une utilisation autre des renseignements recueillis sans obtenir un consentement préalable, dans l'un ou l'autre des cas suivants : 1) si l'utilisation des renseignements est nécessaire aux

fins de fournir la prestation d'un service demandé par la personne concernée; et 2) si l'utilisation des renseignements est manifestement au bénéfice de la personne concernée.

#### Exceptions pour la communication d'un renseignement, sans le consentement de la personne concernée

La Législation québécoise prévoit qu'un renseignement personnel ne peut être communiqué à autrui, sauf en obtenant le consentement de la personne concernée, mais elle prévoit aussi deux exceptions à ce principe.

Les organisations visées par la Législation québécoise peuvent communiquer des renseignements personnels qu'elles ont recueillis, à toute personne ou à tout organisme si cette communication est nécessaire à l'exercice d'un mandat ou à l'exécution d'un contrat de service ou d'entreprise qu'elles confient à cette personne ou à cet organisme. Toutefois, deux conditions doivent alors s'appliquer : 1) le mandat ou le contrat doit être mis par écrit; et 2) parmi les dispositions de tel mandat ou contrat, il faut prévoir les mesures que le mandataire ou l'exécutant du contrat doit prendre pour assurer la protection du caractère confidentiel de ces renseignements.

Les organisations visées par la Législation québécoise peuvent aussi communiquer un renseignement personnel s'il est nécessaire aux fins de la conclusion d'une transaction commerciale. Le récipiendaire de tel renseignement doit alors convenir de l'utiliser uniquement aux fins de la conclusion de cette transaction et de ne pas le communiquer sans avoir obtenu un consentement au préalable ou seulement si la Législation québécoise le prévoit ou l'exige.

#### **Impact de la Législation québécoise sur le personnel**

Selon la Législation québécoise, un renseignement personnel n'est accessible, sans obtenir le consentement de la personne concernée, aux membres du personnel d'une organisation visée par la Législation québécoise qui ont qualité pour connaître tel renseignement qu'à la seule condition que ce renseignement soit nécessaire à l'exercice de leurs fonctions. La Législation québécoise restreint ainsi l'utilisation des renseignements personnels.

## **PARTIE 2**

### **ÉLÉMENTS DE LA LÉGISLATION QUÉBÉCOISE S'APPLIQUANT À L'ORGANISATION**

Il est entendu que l'Organisation recueille, détient et conserve les renseignements personnels de ses clients, des renseignements considérés généralement comme sensibles; elle peut aussi communiquer parfois ces renseignements afin de fournir les produits et/ou services demandés.

L'Organisation ne peut recueillir que les renseignements nécessaires à l'exécution de ses travaux ou ses services pour ses clients et de plus, elle ne peut les utiliser qu'aux fins pour lesquelles ils ont été recueillis, sous réserve de toute exception pouvant s'appliquer.

L'Organisation détient des dossiers numériques, lesquels sont conservés sur un logiciel d'exploitation d'étude notariale géré par un fournisseur autorisé par la Chambre des notaires du Québec. L'Organisation possède aussi une voûte matérielle où se retrouvent des dossiers de ses clients.

L'Organisation doit et a désigné un Responsable qui doit voir à la protection des renseignements recueillis auprès de ses clients et rendre accessibles le titre et les coordonnées du Responsable.

L'Organisation doit établir et implanter des politiques et des pratiques approuvées par le Responsable afin d'encadrer sa gouvernance à l'égard des renseignements personnels de ses clients et rendre accessibles ces politiques à ses clients.

L'Organisation doit informer, lors de la collecte de renseignements, toute personne concernée des éléments suivants: 1) les fins pour lesquelles ses renseignements sont recueillis; 2) les moyens par lesquels ceux-ci sont recueillis; 3) ses droits d'accès et de rectification concernant ses renseignements; et 4) son droit de retirer son consentement à la communication ou à l'utilisation de ses renseignements.

Ainsi selon les différents services offerts par l'Organisation, cette dernière doit **notamment** recueillir verbalement, par le biais d'un échange en vidéoconférence ou téléphonique, ou par écrit, par le biais d'un courriel, d'un courriel sécurisé ou d'un formulaire électronique sécurisé, les renseignements suivants :

### **Matières successorales**

Les renseignements personnels relatifs au défunt, à son conjoint, aux héritiers ou successibles et aux liquidateurs pourront être utilisés par l'Organisation pour les fins suivantes et communiquer aux tiers ci-après définis dans les situations ci-après décrites, sans y être toutefois limitées :

- Recherche testamentaire au Registre des testaments de la Chambre des Notaires du Québec et au Registre des testaments du Barreau du Québec (nom du défunt, sa date de naissance, sa date de décès, son numéro d'assurance sociale, son adresse au décès, ses adresses antérieures, son occupation, son état civil, le nom du conjoint et/ou des ex-conjoint, la date de l'union et/ou du divorce)
- Directeur de l'état civil (nom de la personne, date et lieu de naissance, date et lieu de décès, adresse, nom des parents, nom du conjoint, nom des parents du conjoint, date de naissance du conjoint, date et lieu de mariage)
- Registre des droits personnels et réels mobiliers lors de la publication des avis requis par la Loi ou lors de la consultation du registre (nom du défunt, sa date de naissance, nom des liquidateurs, leur date de naissance, noms des héritiers, leur date de naissance, adresse de la personne qui conservera l'inventaire)
- Journal lors de la publication d'un avis de clôture d'inventaire (nom du défunt, son adresse, sa date de décès, nom des liquidateurs, adresse de la personne qui conservera l'inventaire)
- Registre foncier lors de la publication d'une déclaration de transmission ou autre (nom du défunt, son adresse, sa date de décès, son lieu de décès, son occupation, son état matrimonial, nom des liquidateurs, leur occupation et leur adresse, nom des héritiers et leur adresse)

### **Testaments et mandats**

Les renseignements personnels du client pourront être utilisés par l'Organisation pour les fins suivantes et partagées à la Chambre des notaires :

- Inscription du testament au Registre des testaments et du mandat de protection au Registre des mandats de la Chambre des Notaires du Québec (nom, adresse, numéro d'assurance-maladie, numéro d'assurance sociale, état civil, consentement ou refus du don d'organes)

### **Directives médicales anticipées**

Les renseignements personnels du client pourront être utilisés par l'Organisation pour les fins suivantes :

- Publication de l'acte au long au Registre de la Régie de l'assurance-maladie du Québec (lequel inclus le nom, l'occupation, l'adresse, le numéro d'assurance-maladie du Québec, et les volontés du client)

### **Procédures non contentieuses**

Les renseignements personnels de la personne concernée, ou du défunt, des demandeurs, des personnes intéressées et des personnes devant ou pouvant être convoquées à l'assemblée de parents, d'alliés et d'amis, le cas échéant, pourront être utilisés par l'Organisation pour les fins suivantes :

- Dans les actes de procédures lesquels seront signifiés et/ou notifiés à la personne concernée, aux personnes intéressées, aux personnes pouvant ou devant être convoquées à l'assemblée de parents, d'alliés et d'amis, au Curateur Public du Québec, à l'huissier de justice et à la Cour concerné :
  - o Pour la personne concernée : nom, occupation, adresse, état civil, date de naissance, nom de ses descendants, de son conjoint, de ses parents, de sa fratrie, diagnostic et informations quant à sa capacité, selon la procédure concernée ;
  - o Pour les demandeurs, les personnes intéressées, les personnes devant ou pouvant être convoquées à l'assemblée de parents, d'alliés et d'amis, ou tout autre intervenant requis : nom, occupation, adresse, adresse courriel, lien avec la personne concernée ;
  - o Pour le défunt : nom, occupation, adresse, état civil, informations relatives à son testament olographe ou devant témoins et aux volontés qui y sont décrites.

Des renseignements personnels pourront également être recueillis et partagés avec le travailleur social mandaté dans le cadre d'une homologation de mandat ou de l'ouverture d'une mesure de protection.

### **Matières immobilières**

Les renseignements personnels des acheteurs, des vendeurs ou de tout autre partie concernée par un transfert immobilier pourront être utilisés par l'Organisation pour les fins suivantes :

- Acte notarié (hypothèque, vente ou autre type de transfert immobilier) : nom, occupation, adresse et état civil de chacune des parties ainsi que des copies de deux pièces d'identité, coordonnées bancaires des vendeurs et des acheteurs, le cas échéant;
- Institutions financières concernées : noms, adresses, informations relatives aux garanties hypothécaires et tout autre emprunt devant être remboursé.

Dans le cadre d'une transaction immobilière, certaines informations seront partagées avec des tiers afin de veiller au bon déroulement de la transaction, plus particulièrement les noms et adresses des parties non seulement à l'institution financière concernée, mais également auprès du Registre des droits

personnels et réels mobiliers pour fins de publication d'hypothèque mobilière, Assyst Immobilier, Assyst Paiement, Stewart Title Guaranty Co.

### **Autres matières familiales**

Les renseignements personnels des conjoints/futurs époux pourront être utilisés par l'Organisation pour les fins suivantes :

- Acte notarié : nom, occupation, adresse, état civil, nom des parents, numéro d'assurance sociale (seulement en cas de donation)
- Inscription d'un mariage : nom, adresse, numéro de téléphone, date de naissance, état civil, date et lieu du mariage, nombre d'années de scolarité, langue maternelle, âge, nom des parents, nom des témoins)

### **Matières corporatives**

Les renseignements personnels suivants pourront être recueillis par l'Organisation afin d'accomplir son mandat:

Incorporation: 1) prénom, nom, adresse des fondateurs, des administrateurs, des actionnaires et des bénéficiaires ultimes. 2) Pièce d'identité des administrateurs pour vérification de l'identité et transmission auprès du Registraire des entreprises du Québec, le cas échéant, pour se conformer aux exigences de la *Loi sur la publicité légale des entreprises*. 3) Date de naissance des administrateurs et des bénéficiaires ultimes, adresse de la société à créer, activité(s) de l'entreprise. 4) Tous renseignements nécessaires à l'incorporation seront déterminés suivant la situation spécifique de la personne concernée et transmise, lorsque nécessaire, auprès du Registraire des entreprises.

Mises à jour annuelles: 1) prénom, nom des administrateurs et des actionnaires pour la période en cours. 2) Consultation des états financiers de l'entreprise 3) Consultation du livre de la société afin d'en faire un examen. Tous autres renseignements nécessaires ou utiles seront déterminés suivants les caractéristiques spécifiques du mandat.

### **Fiducies**

Les renseignements personnels suivants pourront être recueillis par l'Organisation afin d'accomplir son mandat:

- Prénom, nom, adresse et occupation des constituants et des fiduciaires et des bénéficiaires;
- Date de naissance des constituants et des bénéficiaires;
- Numéro d'assurance sociale du ou des bénéficiaires, le cas échéant.

Les listes de renseignements personnels décrites ci-avant ne sont pas exhaustives, mais ont été intégrées à la présente politique afin de présenter en termes clairs et avec un souci de transparence les fins de leur obtention, de leur utilisation et de leur partage, le cas échéant, par l'Organisation.

Chaque personne pour laquelle des renseignements personnels ont été recueillis pourra en tout temps :

1) avoir accès aux renseignements ainsi recueillis 2) Faire une demande de rectification 3) Retirer son consentement à la communication ou à l'utilisation de ses renseignements (sauf exceptions prévues aux termes de notre *Politique concernant la protection des renseignements personnels*)

En prévision de la possibilité qu'un incident de confidentialité se produise, l'Organisation doit prévoir les mesures raisonnables pour diminuer les risques qu'un préjudice soit causé suite à un tel incident et tenir un registre des incidents de confidentialité.

L'Organisation bénéficie d'une exception pour une utilisation autre des renseignements personnels recueillis sans obtenir le consentement des personnes concernées, à la condition que telle utilisation soit nécessaire pour fournir la prestation d'un service au client ou à la condition que telle utilisation soit au bénéfice du client.

L'Organisation peut communiquer les renseignements personnels de ses clients à toute personne ou organisme si cela est nécessaire à : 1) l'exercice d'un mandat ou à l'exécution d'un contrat de service ou d'entreprise qu'elle leur confie, pourvu que l'Organisation respecte deux conditions : le mandat ou le contrat confié est mis par écrit et il prévoit les mesures que le mandataire ou l'exécutant du contrat doit prendre pour assurer la protection du caractère confidentiel des renseignements transmis; et 2) la conclusion d'une transaction commerciale.

L'Organisation ne pourra, sans obtenir le consentement des personnes concernées, rendre accessibles des renseignements personnels aux membres de son personnel ayant qualité pour les connaître qu'à la seule condition que ces renseignements soient nécessaires à l'exercice de leurs fonctions.

### **PARTIE 3**

#### **MESURES DE L'ORGANISATION POUR SE CONFORMER À LA LÉGISLATION QUÉBÉCOISE**

→ *Mesures déjà mises en oeuvre*

L'Organisation a déjà mis en oeuvre l'une ou l'autre des mesures mentionnées ci-dessous pour se conformer aux dispositions de la Législation québécoise et ce, aux fins d'assurer la protection et la confidentialité des renseignements personnels de ses clients. Certaines mesures peuvent être d'ordre général et d'autres d'ordre spécifique.

Désigner la plus haute autorité de l'Organisation comme étant le Responsable, laquelle a délégué par écrit cette fonction à une autre personne au sein de l'Organisation, soit M<sup>e</sup> Roxanne Duhaime, notaire, et rendre accessibles à ses clients le nom, le titre et les coordonnées du Responsable et en faire la publication auprès de ses clients ou sur le site web de l'Organisation, le cas échéant.

Établir des protocoles de communication sécuritaires standardisés et des mesures de sécurité notamment un processus de chiffrement ou d'encryptage s'appliquant lors de la transmission à des tiers de renseignements personnels appartenant à des clients de l'Organisation, le cas échéant.

Déterminer la transmission des renseignements personnels des clients de l'Organisation auprès de

quels types de sociétés ou d'entreprises (fournisseurs, sous-contractants, etc.) et à quels endroits à l'extérieur du Québec.

Déterminer les renseignements à recueillir qui sont nécessaires à l'exécution de ses travaux ou ses services pour ses clients et utilisés qu'aux seules fins pour lesquelles ils ont été recueillis et établir des mesures de contrôle à cet effet.

Déterminer toute situation nécessitant la communication des renseignements personnels de ses clients à toute personne ou organisme ainsi que les conditions applicables à telle communication et voir à faire signer une entente à ces personnes ou organismes.

Faire signer à toute personne recevant des renseignements personnels des clients de l'Organisation une entente de confidentialité s'appliquant aux renseignements transmis et prévoyant les mesures à prendre pour en protéger la confidentialité.

Communiquer, sans le consentement préalable du client, des renseignements recueillis si cela est nécessaire pour conclure une transaction commerciale, le récipiendaire des renseignements devant convenir de les utiliser que pour cette transaction et de ne pas les communiquer à son tour sans un consentement préalable.

→ *Mesures à mettre en oeuvre*

L'Organisation verra à mettre en oeuvre dans les meilleurs délais l'une ou l'autre des mesures mentionnées ci-dessous pour se conformer aux dispositions de la Législation québécoise et ce, aux fins d'assurer la protection et la confidentialité des renseignements personnels de ses clients. Certaines mesures peuvent être d'ordre général et d'autres d'ordre spécifique.

Déterminer les principaux éléments et voir à la préparation et la rédaction des politiques et des pratiques en lien avec la protection des renseignements personnels de ses clients qui doivent être approuvées par le Responsable, en vue de leur mise en oeuvre au sein de l'Organisation. Rendre ces politiques et pratiques accessibles auprès de ses clients. Préparer un résumé de ces politiques et pratiques pour ses clients afin de leur remettre en personne ou leur envoyer par courriel ou le publier sur le site web de l'Organisation, le cas échéant. Ces politiques et pratiques servent notamment d'encadrement pour la conservation et la destruction des renseignements de ses clients, pour les rôles et les responsabilités des membres de son personnel tout au long du cycle de vie de ces renseignements et pour un processus visant le traitement des plaintes en relation avec la protection des renseignements de ses clients.

Déterminer les différents points à soumettre verbalement à chaque client de l'Organisation lors de la collecte de ses renseignements, pour l'informer des éléments suivants : 1) les fins pour lesquelles ses renseignements sont recueillis; 2) les moyens par lesquels ceux-ci sont recueillis; 3) ses droits d'accès et de rectification concernant ses renseignements; et 4) son droit de retirer son consentement à la communication ou à l'utilisation de ses renseignements.

Voir à la préparation et la rédaction de modèles pour les ententes requises aux fins de bénéficier de certaines exemptions prévues par la Législation québécoise concernant l'obtention préalable du consentement d'une personne concernée.

Divulguer tout incident de confidentialité à la personne concernée et la Commission d'accès à l'information par l'envoi d'un avis écrit.

Advenant un incident de confidentialité, mettre en place des mesures pour diminuer les risques qu'un préjudice soit causé.

Tenir un registre des incidents de confidentialité pour prendre en compte les cas où de tels incidents pourraient se produire, selon le contenu de ce registre établi par règlement et par la suite, tenir ce registre à jour. Advenant l'avènement de tout tel incident, l'Organisation doit en aviser par écrit la Commission d'accès à l'information du Québec et toute personne concernée, selon le contenu de ces avis établi par règlement.

Déterminer les fins pour lesquelles l'Organisation peut recueillir des renseignements auprès de ses clients.

→ *Mesures que l'Organisation n'entend pas mettre en oeuvre*

L'Organisation n'entend pas mettre en oeuvre l'une ou l'autre des mesures mentionnées ci-dessous. Certaines mesures peuvent être d'ordre général et d'autres d'ordre spécifique.

Déterminer le délai de conservation des renseignements personnels des clients de l'Organisation et lorsque nécessaire, établir un calendrier de conservation pour mieux les gérer. Considérant que l'Organisation a pour vocation d'assurer la pérennité d'actes notariés plusieurs renseignements personnels doivent être conservés sans date ni calendrier de destructions applicables;

Déterminer toute situation nécessitant une utilisation autre par l'Organisation des renseignements recueillis auprès de ses clients, sans obtenir le consentement des personnes concernées.

Communiquer à des tiers, sans le consentement préalable du client, des renseignements recueillis si cela est nécessaire à l'exécution d'un mandat ou d'un contrat de service ou d'entreprise si tel mandat ou contrat est par écrit et prévoit les mesures à prendre pour en protéger la confidentialité. Le consentement du client est requis lors de la communication à un tiers.

## **PARTIE 4**

### **MESURES DE L'ORGANISATION POUR SON SYSTÈME INFORMATIQUE**

Il est reconnu qu'un système informatique performant et efficace assure beaucoup mieux la protection de la confidentialité des renseignements personnels des clients de toute organisation visée par la Législation québécoise.

→ *Mesures déjà mises en oeuvre*

L'Organisation ou son ou ses fournisseurs informatiques ont déjà mis en oeuvre l'une ou l'autre des mesures mentionnées ci-dessous pour se doter d'un système informatique performant et bien gérer les renseignements personnels y contenus ainsi que son personnel y ayant accès.

Gérer les accès des membres de son personnel à son système informatique, en utilisant des mesures simples mais efficaces pour assurer cette gestion.

S'assurer qu'il y a des mesures de sécurité requises pour accéder à son système informatique, notamment des mots de passe, et mettre en place un mécanisme pour déterminer les accès sécurisés à son système informatique.

Déterminer les niveaux de sécurité requis pour chacun des membres de son personnel ayant accès à son système informatique.

Déterminer le mode de fonctionnement des mots de passe utilisés par les membres de son personnel accédant à son système informatique et voir à ce que ces membres le respectent en établissant des mesures de contrôle.

Établir un accès sélectif aux données sur son système informatique pour les membres de son personnel qui ont été autorisés uniquement.

Établir les mesures de protection devant s'appliquer à son système informatique en lien avec les renseignements personnels de ses clients recueillis et conservés.

Nommer une personne chargée de la mise en oeuvre pour son système informatique des mesures de protection des renseignements personnels de ses clients.

Déterminer les membres de son personnel responsables de l'inventaire des renseignements personnels de ses clients.

Utiliser et mettre à jour des anti-virus et des anti-logiciels espions sur son système informatique.

Utiliser des équipements « coupe-feu » sur son système informatique pour éviter toute intrusion non contrôlée provenant de l'Internet.

Utiliser des mécanismes de fin de session automatique pour désactiver au besoin toute connexion inactive avec l'Internet pendant un certain temps.

→ *Mesures à mettre en oeuvre*

L'Organisation ou son ou ses fournisseurs informatiques verront à mettre en oeuvre dans les meilleurs délais l'une ou l'autre des mesures mentionnées ci-dessous pour être en mesure de se doter d'un système informatique performant et de bien gérer les renseignements personnels y contenus ainsi que son personnel y ayant accès.

Établir les tâches et responsabilités des membres de son personnel s'occupant, au niveau de son système informatique, de la protection des renseignements personnels de ses clients et ce, tout au long du cycle de vie de ces renseignements.

Tenir des activités de formation traitant de la protection des renseignements personnels de ses clients pour les membres de son personnel s'occupant, au niveau de son système informatique, de la protection de ces renseignements.

Établir une liste exhaustive (inventaire) des renseignements personnels de ses clients recueillis et détenus.

Utiliser un procédé de chiffrement sécuritaire des données, c'est-à-dire encrypter les renseignements personnels de ses clients.

Demander à son personnel autorisé à accéder aux renseignements personnels de ses clients de vider la mémoire cache de leur fureteur afin d'éviter que les informations sur toute session précédente tombent sous des regards indiscrets.

Posséder des mécanismes offrant une protection des données, notamment contre l'accès non autorisé aux renseignements personnels.

→ *Mesures que l'Organisation n'entend pas mettre en oeuvre*

Même si un système informatique performant assure une meilleure protection de la confidentialité des renseignements personnels, l'Organisation ou son ou ses fournisseurs informatiques n'entendent pas mettre en oeuvre l'une ou l'autre des mesures mentionnées ci-dessous.

Établir des restrictions pour que seulement son personnel autorisé puisse accéder à certains de ses équipements informatiques identifiés au préalable.

Établir une méthodologie pour déterminer les dossiers actifs et les dossiers inactifs de l'Organisation et mettre en place un mécanisme pour distinguer les dossiers selon l'un de ces deux types.

## **PARTIE 5**

### **ÉTABLIR UNE LISTE (INVENTAIRE) DES RENSEIGNEMENTS PERSONNELS RECUEILLIS PAR L'ORGANISATION**

Il est important pour l'Organisation de comprendre et gérer au mieux le flux des renseignements personnels qu'elle recueille auprès de ses clients et ce, pour en assurer la protection de manière efficace, facile et rapide.

Pour ce faire, il est important pour l'Organisation d'établir une liste exhaustive (inventaire) des renseignements personnels qu'elle recueille et détient, ce qui lui permet de s'assurer qu'aucun de ces renseignements n'entre ou ne sort de son système sans être recensé; l'Organisation pourra alors démontrer facilement qu'elle a adopté une culture du respect de la vie privée, incluant la protection des renseignements personnels. Une telle liste peut aussi lui devenir très utile lors des évaluations des facteurs relatifs à la vie privée que l'Organisation peut être appelée à faire.

En effet, si l'Organisation ne comprend pas le flux des renseignements qu'elle recueille, il devient difficile de savoir que ses activités sont conformes aux dispositions de la Législation québécoise.

Pour bâtir cette liste exhaustive, l'Organisation doit tout d'abord choisir l'approche à adopter et le format à privilégier.

## **Processus pour établir la liste exhaustive des renseignements personnels recueillis**

L'Organisation doit déterminer la source principale à partir de laquelle les renseignements personnels sont recueillis et en faire une liste exhaustive (inventaire) tout en établissant si ces renseignements sont de nature sensible ou non; elle doit aussi déterminer à quel endroit ces renseignements sont conservés. L'Organisation doit ensuite associer les renseignements contenus dans cette liste exhaustive aux consentements qu'elle a obtenus aux fins d'en faire la collecte, l'utilisation et la transmission; par la suite, elle doit aussi établir les objectifs poursuivis en vue d'en faire la collecte, l'utilisation et la transmission.

Ce processus implique également ce qui suit pour l'Organisation : 1) déterminer le délai de conservation de ces renseignements et si possible, établir un calendrier de conservation pour en assurer une meilleure gestion; 2) choisir les mesures de sécurité permettant de protéger adéquatement ces renseignements, en fonction notamment de leur niveau de sensibilité; et 3) établir à qui ou à quels endroits ces renseignements sont transmis, en tenant compte des endroits géographiques concernés et tout en mettant en place des protocoles applicables lors de leur transmission auprès de tiers afin de mieux les protéger.

L'Organisation doit également déterminer les membres de son personnel responsables d'établir cette liste exhaustive, les moyens automatisés à utiliser pour l'établir et déterminer une stratégie de mise à jour de celle-ci.

## **Mesures de l'Organisation pour une liste exhaustive des renseignements personnels**

→ *Mesures déjà mises en oeuvre*

L'Organisation ou son ou ses fournisseurs informatiques ont déjà mis en oeuvre l'une ou l'autre des mesures mentionnées ci-dessous concernant la liste exhaustive des renseignements personnels qu'elle recueille et détient.

Déterminer où conserver les renseignements répertoriés.

Établir le délai de conservation des renseignements répertoriés et le cas échéant, prévoir un calendrier de conservation.

Confirmer les emplacements où se fait la transmission des renseignements répertoriés.

Déterminer des protocoles pour protéger les renseignements personnels lors de leur transmission auprès de tiers.

Déterminer les seuls membres de son personnel pouvant accéder aux renseignements sensibles des clients et à ceux contenus dans le système informatique.

→ *Mesures à mettre en oeuvre*

L'Organisation verra à mettre en oeuvre dans les meilleurs délais l'une ou l'autre des mesures mentionnées ci-dessous concernant la liste exhaustive des renseignements personnels qu'elle recueille

et détient.

Déterminer les mesures de sécurité appropriées pour la protection des renseignements répertoriés.

Établir les mesures de sécurité s'appliquant spécifiquement aux renseignements sensibles de ses clients afin de les protéger adéquatement.

Établir la liste exhaustive (inventaire) de tous les renseignements personnels et données recueillis et les associer aux consentements déjà obtenus, le cas échéant.

Déterminer à quels endroits géographiques se fait la communication des renseignements répertoriés.

## **PARTIE 6**

### **MESURES DE L'ORGANISATION POUR SON PERSONNEL**

→ *Mesures déjà mises en oeuvre*

L'Organisation a déjà mis en oeuvre l'une ou l'autre des mesures mentionnées ci-dessous pour bien gérer son personnel ayant notamment accès aux renseignements personnels de ses clients.

Déterminer les membres de son personnel ayant qualité pour connaître les renseignements personnels de ses clients, en faisant abstraction des renseignements sensibles.

Faire signer des ententes de confidentialité à tous les membres de son personnel ayant accès, régulièrement ou non, aux renseignements personnels de ses clients.

Mettre en place un mécanisme pour gérer les autorisations de son personnel accédant aux renseignements personnels de ses clients.

Déterminer et appliquer des mesures de contrôle s'appliquant à son personnel qui est autorisé à accéder aux renseignements personnels de ses clients.

Déterminer les membres de son personnel en charge de la conservation et de la destruction des renseignements personnels de ses clients.

Rendre accessibles, sans obtenir le consentement des personnes concernées, les renseignements personnels de ses clients aux membres de son personnel ayant qualité pour les connaître seulement si ces renseignements sont nécessaires à l'exercice de leurs fonctions et établir des mesures de contrôle pour un tel accès.

Faire des enquêtes ou des vérifications de pré-emploi avant l'embauche de tout membre de son personnel.

## **PARTIE 7**

### **MESURES DE L'ORGANISATION POUR SON SITE WEB**

→ *Mesure à mettre en oeuvre*

L'Organisation ou son ou ses fournisseurs informatiques verront à mettre en oeuvre dans les meilleurs délais l'une ou l'autre des mesures mentionnées ci-dessous pour être en mesure de bien gérer son site web.

Sécuriser les pages de son site web pour assurer la protection des renseignements transmis sur son site web par ses clients.

→ *Mesure que l'Organisation ou son ou ses fournisseurs informatiques n'entendent pas mettre en oeuvre*

L'Organisation ou son ou ses fournisseurs informatiques n'entendent pas mettre en oeuvre l'une ou l'autre des mesures mentionnées ci-dessous concernant un site.

Sécuriser les pages de son site web pour assurer la protection des renseignements transmis sur son site web par ses clients.

Utiliser des certificats de chiffrement de données (encryptage) pour assurer la codification de tous les renseignements personnels inscrits sur son site web.

## **PARTIE 8**

### **MESURES DE L'ORGANISATION QUI EST OBLIGÉE D'AVOIR UNE VOÛTE MATÉRIELLE**

→ *Mesures déjà mises en oeuvre*

L'Organisation a déjà mis en oeuvre l'une ou l'autre des mesures mentionnées ci-dessous concernant la voûte matérielle qu'elle possède.

Sécuriser les pages de son site web pour assurer la protection des renseignements transmis sur son site web par ses clients.

Assurer le verrouillage adéquat de la voûte matérielle.

Déterminer les membres de son personnel ayant accès à la voûte matérielle et leur accorder des codes de sécurité pour y accéder.

Déterminer un membre de son personnel ayant la responsabilité de la voûte matérielle.

Déterminer les mesures pour assurer la protection des renseignements personnels de ses clients se

trouvant dans la voûte matérielle.

Établir les protocoles nécessaires pour accéder à la voûte matérielle et les maintenir à jour.

Déterminer les mesures de sécurité et de contrôle applicables pour assurer la confidentialité des données se trouvant dans la voûte matérielle et voir à leur mise en oeuvre et leur maintien à jour.

Sécuriser les pages de son site web pour assurer la protection des renseignements transmis sur son site web par ses clients.

Sécuriser les pages de son site web pour assurer la protection des renseignements transmis sur son site web par ses clients.



Approuvé par l'Organisation en date du 21 septembre 2023.

*(Signé Me Roxanne Duhaime, notaire)*  
*Nom et signature de responsable pour l'Organisation*