



POLITIQUE DE PROTECTION DES RENSEIGNEMENTS PERSONNELS

RÉSEAU NOTARIAL PLUS

Version:	1.0
Date de version	21 mai 2024
Créé	Raymond Chabot Grant Thornton & Cie S.E.N.C.R.L.
Approuvé par	
Niveau de confidentialité	Confidentiel

Historique des modifications

Date	Version	Auteur(s)	Description des modifications
21/05/2024	1.0	Raymond Chabot Grant Thornton & Cie S.E.N.C.R.L.	Création du document de base.

Table des matières

1.OBJET ET PORTÉE DE LA POLITIQUE.....	3
2.DOCUMENTS DE RÉFÉRENCE.....	4

LÉGISLATION PERTINENTE	4
AUTRES DOCUMENTS.....	5
3.DÉFINITIONS.....	5
4.PRINCIPES GÉNÉRAUX.....	7
RESPONSABILISATION ET GOUVERNANCE.....	7
CONSENTEMENT.....	7
ÉQUITÉ ET LÉGALITÉ.....	7
TRANSPARENCE.....	7
DÉTERMINER LES FINS DE LA COLLECTE ET DE L'UTILISATION.....	8
LIMITATION DE LA COLLECTE ET DE L'UTILISATION.....	8
EXACTITUDE ET RECTIFICATION.....	8
CONSERVATION ET ANONYMISATION.....	8
SÉCURITÉ ET CONFIDENTIALITÉ.....	9
5.INTÉGRATION DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS AUX ACTIVITÉS COMMERCIALES.....	9
NOTIFICATION AUX PERSONNES CONCERNÉES.....	9
CHOIX ET CONSENTEMENT DE LA PERSONNE CONCERNÉE.....	9
COLLECTE DE RENSEIGNEMENTS PERSONNELS.....	9
UTILISATION, CONSERVATION ET DESTRUCTION.....	9
DIVULGATION À DES TIERS.....	10
DIVULGATION DANS LE CADRE D'UNE TRANSACTION COMMERCIALE.....	11
TRANSFERT À L'EXTÉRIEUR DU QUÉBEC.....	11
DROIT D'ACCÈS ET RECTIFICATION	11
DROIT À LA PORTABILITÉ.....	12
DROIT À LA DÉINDEXATION.....	12
6.LIGNES DIRECTRICES POUR UN TRAITEMENT ÉQUITABLE.....	12
DROIT D'ÊTRE INFORMÉ DES PERSONNES CONCERNÉES.....	12
OBTENIR LES CONSENTEMENTS.....	13
7.ORGANISATION ET GOUVERNANCE.....	14
8.SIGNALEMENT ET RÉPONSE AUX INCIDENTS DE CONFIDENTIALITÉ.....	15
9.AUDIT	15
10.SANCTIONS.....	15
11.CONFLITS.....	16
12.GESTION DOCUMENTAIRE.....	16
13.VALIDITÉ	17

1. Objet et portée de la Politique

Réseau Notarial Plus (la « **Société** ») est engagée à respecter la vie privée de chacun conformément aux lois, règlements et normes applicables en matière de protection des Renseignements personnels. La présente politique de protection des Renseignements personnels (la « **Politique** ») a pour objectif d'énoncer les principes généraux auxquels la Société adhère ainsi que les pratiques que nous mettons en œuvre lorsque nous recueillons, utilisons, communiquons, conservons, détruisons les Renseignements personnels de nos clients, fournisseurs, partenaires commerciaux, employés et autres personnes concernées, dans le cadre de nos activités. Cette Politique présente également les responsabilités qui incombent aux différents comités et aux cadres de la Société.

La présente Politique s'applique à tous ses employés, comités, fournisseurs de services, partenaires commerciaux et autres contractants qui travaillent pour le compte ou avec la Société.

2. Documents de référence

Législation pertinente

! *Loi sur la protection des renseignements personnels dans le secteur privé*, RLRQ c P-39.1 (la « **Loi sur le secteur privé** »);

! *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*, LQ 2021 c 25 (la « **Loi 25** », sanctionnée le 22 septembre 2021);

! *Loi visant à promouvoir l'efficacité et la capacité d'adaptation de l'économie canadienne par la réglementation de certaines pratiques qui découragent l'exercice des activités commerciales par voie électronique et modifiant la Loi sur le Conseil de la radiodiffusion et des télécommunications canadiennes, la Loi sur la concurrence, la Loi sur la protection des renseignements personnels et les documents électroniques et la Loi sur les télécommunications (Loi anti-pourriels)*, LC 2010 c 23;

! *Loi concernant le cadre juridique des technologies de l'information*, RLRQ c C-1.1;

! *Charte des droits et libertés de la personne*, RLRQ c C-12;

! *Code civil du Québec*, RLRQ c CCQ-1991;

(collectivement, les « **Lois sur la protection de la vie privée** »)

Autres documents

- ! Politique de protection des renseignements personnels des employés;
- ! Politique de confidentialité (site Web);
- ! Description du poste de Responsable à la protection des renseignements personnels;
- ! Lignes directrices pour répertorier les activités de traitement des Renseignements personnels;
- ! Procédure de demande d'accès et de rectification;
- ! Méthodologie d'évaluation des facteurs relatifs à la vie privée;
- ! Lignes directrices dans le cadre des évaluations des facteurs relatifs à la vie privée;
- ! Registre des évaluations des facteurs relatifs à la vie privée;
- ! Procédure de transfert de Renseignements personnels hors Québec;
- ! Questionnaire de conformité des fournisseurs avec les Lois québécoises sur la protection de la vie privée;
- ! Politique d'anonymisation et dépersonnalisation;
- ! Procédure de réponse et de notification en cas d'incident de confidentialité;
- ! Analyse de risque de préjudice sérieux pour les personnes concernées;
- ! Registre des incidents de confidentialité.

3. Définitions

Les mots et expressions qui suivent, lorsqu'ils apparaissent avec une première lettre en majuscule dans la Politique, ont le sens qui leur est attribué ci-après, à moins d'une dérogation implicite ou explicite dans le texte :

Activité de traitement ou Traitement : désigne toute opération ou ensemble d'opérations effectuées sur des renseignements personnels ou des ensembles de renseignements personnels, que ce soit ou non par des moyens automatisés, telles que la collecte, l'enregistrement, l'organisation, la structuration, le stockage, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la divulgation par transmission, diffusion ou toute autre forme de mise à disposition, l'alignement ou la combinaison, la restriction, l'effacement ou la destruction.

Anonymiser : signifie tout moyen permettant de faire en sorte qu'un renseignement concernant un individu ne permette plus, de façon irréversible, d'identifier directement ou indirectement cette personne, le tout selon les meilleures pratiques généralement reconnues.

Dépersonnalisation : signifie toute méthode, incluant la suppression des noms et identifiants évidents, permettant de faire en sorte qu'un renseignement personnel ne permette plus d'identifier directement la personne concernée.

Évaluation des facteurs relatifs à la vie privée ou ÉFVP : désigne le processus conçu pour décrire les activités de traitement, évaluer la nécessité et la proportionnalité d'un traitement et aider à gérer les risques pour les droits et libertés des personnes physiques résultant du traitement des Renseignements personnels.

Incident de confidentialité : désigne 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 ou à son caractère confidentiel.

Renseignements personnels : désigne tout renseignement qui concerne une personne physique et permet de l'identifier, c'est-à-dire qui révèle de manière directe ou indirecte ou par référence, quelque chose sur l'identité, les caractéristiques, les activités, l'emplacement ou d'autres informations identifiables (ex. : habiletés, préférences, tendances psychologiques, prédispositions, capacités mentales, caractère et comportement, situation économique culturelle ou sociale) de cette personne, et ce quelle que soit la nature du support et quelle que soit la forme sous laquelle ces renseignements sont accessibles (écrite, graphique, sonore, visuelle, informatisée ou autre) et inclus dans tous les cas, un Renseignement personnel sensible.

À titre d'exemples, sont considérés comme des Renseignements personnels :

- ! Le nom, prénom et pseudonyme d'une personne ;
- ! L'âge ;
- ! L'origine ethnique ;
- ! L'adresse civique ;
- ! Le numéro de téléphone ;
- ! L'adresse courriel et les messages ;
- ! L'adresse IP et les données de géolocalisation ;
- ! Le niveau d'éducation ;
- ! Les informations sur la vie personnelle ;
- ! L'état matrimonial ;
- ! Les renseignements relatifs à un travail et aux antécédents professionnels, incluant les renseignements traduisant l'appréciation du travail par des supérieurs ou collègues de travail ;
- ! Les renseignements relatifs à la vie personnelle de la personne concernée, soit l'inventaire de ses titres de propriété(s), les titres afférents au régime matrimonial (biens meubles et immeubles);
- ! Les renseignements relatifs à la succession de la personne concernée;
- ! Les mots de passe de compte(s) bancaire, d'autres informations financières et mot(s) de passe de portefeuilles de cryptomonnaie;
- ! Le contenu des recherches effectuées en ligne et les préférences d'utilisateur ;
- ! Les données biométriques ;
- ! Les informations bancaires et financières, incluant les relevés fiscaux, les numéros de carte de crédit et de débit ;
- ! Le dossier médical, le numéro d'assurance maladie et les informations sur l'état de santé (ex. : notes, évaluations cliniques et diagnostics) ;
- ! Les relevés de compte de téléphone cellulaire utilisé ou non pour le travail ;
- ! Le numéro d'assurance sociale (NAS), le numéro de permis de conduire, le numéro de passeport ou d'autres identifiants similaires.

Renseignements personnels sensibles : un Renseignement personnel est considéré comme sensible lorsque, 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 respect de la vie privée. Il peut s'agir, par exemple, de renseignements médicaux, biométriques, génétiques ou financiers, ou encore de renseignements sur la vie ou l'orientation sexuelle, les convictions politiques, religieuses ou philosophiques, l'appartenance syndicale ou bien l'origine ethnique.

Responsable de la protection des renseignements personnels : désigne la personne qui veille à assurer le respect et la mise en œuvre des Lois sur la protection de la vie privée au sein de la Société.

4. Principes généraux

Les Lois sur la protection de la vie privée ainsi que certains contrats avec laquelle la Société est liée obligent la Société à se conformer aux principes généraux suivants :

Responsabilisation et gouvernance

La Société est responsable de la protection des Renseignements personnels qu'elle détient, utilise, traite, communique, conserve ou détruit. Elle doit entre autres :

- ! Désigner une personne chargée d'assurer le respect et la mise en œuvre des Lois sur la protection de la vie privée, incluant les principes énoncés ci-dessous;
- ! Établir et mettre en œuvre des politiques et des pratiques encadrant sa gouvernance à l'égard des Renseignements personnels;
- ! Répondre aux demandes d'accès et de rectification qui lui sont transmises;
- ! Publier sur son site Web, son Programme de gouvernance de l'information relatant les politiques et pratiques en vigueur;
- ! Aviser la Commission d'accès à l'information et les personnes concernées de tout Incident de confidentialité.

Consentement

Avant de recueillir, d'utiliser ou de communiquer des Renseignements personnels, la Société doit obtenir un consentement valable de la personne concernée compte tenu du caractère sensible des Renseignements personnels en cause. Ce consentement doit être manifeste, libre, éclairé et être donné à des fins spécifiques. Il doit être demandé pour chacune de ces fins en termes simples et clairs, distinctement de toute autre information communiquée à la personne concernée. En principe, le consentement explicite est la règle tandis que le consentement implicite est l'exception prévue par la Loi.

Le consentement ne vaut que pour la durée nécessaire à la réalisation des fins pour lesquelles il a été demandé. La Société doit obtenir un consentement supplémentaire de la personne concernée pour utiliser les Renseignements personnels visés à une fin secondaire ou autre.

Équité et légalité

Les Renseignements personnels doivent être traités par des moyens équitables et légaux tout au long de leur cycle de vie.

Transparence

La Société doit informer ses clients et ses employés des politiques et des pratiques de gestion des Renseignements personnels qu'elle met en œuvre dans le cadre de ses activités et opérations. Ces politiques et pratiques doivent être rédigées en termes simples et clairs et être faciles d'accès.

Ainsi, avant de recueillir ou au moment de recueillir des Renseignements personnels, la Société doit communiquer aux personnes concernées les informations minimales suivantes :

- ! Les fins légitimes auxquelles ces renseignements sont recueillis;
- ! Les moyens par lesquels les renseignements sont recueillis;
- ! Les droits d'accès et de rectification prévus par la loi;
- ! Le droit pour la personne concernée de retirer son consentement à la communication ou à l'utilisation de ses renseignements;
- ! Le nom du tiers pour qui la collecte est faite, le cas échéant;
- ! La possibilité que les renseignements soient communiqués à l'extérieur du Québec, le cas échéant.

Sur demande de sa part, la personne concernée doit également être informée des éléments suivants :

- ! Les fins pour lesquelles les renseignements ont été collectés;
- ! Les Renseignements personnels recueillis auprès d'elle;
- ! Les catégories de personnes qui ont accès à ces Renseignements personnels au sein de la Société;
- ! La durée de conservation de ces renseignements;
- ! Les coordonnées du Responsable de la protection des Renseignements personnels.

Déterminer les fins de la collecte et de l'utilisation

Les Renseignements personnels doivent être recueillis et utilisés à des fins spécifiques, explicites et légitimes, c'est-à-dire directement liées et manifestement nécessaires à la réalisation des Activités de traitement pour lesquelles ils ont été recueillis. Ces fins doivent être établies avant la collecte et l'utilisation des Renseignements personnels. La Société doit faire preuve d'honnêteté et de transparence au sujet des raisons pour lesquelles elles recueillent des Renseignements personnels.

Limitation de la collecte et de l'utilisation

La Société doit recueillir uniquement des Renseignements personnels nécessaires à la réalisation des fins explicites et légitimes établies, et ne doit pas traiter ces Renseignements personnels ultérieurement d'une manière incompatible avec ces fins déterminées, à moins d'obtenir le consentement de la personne concernée pour utiliser ces Renseignements personnels à une autre fin légitime.

Exactitude et rectification

La Société doit veiller à ce que les Renseignements personnels qu'elle détient soient à jour et exacts au moment où elle les utilise pour prendre une décision relative à la personne concernée. Cette obligation vise à sauvegarder l'intégrité de l'information, tant dans son fond que sa forme, et à s'assurer que la personne concernée ne subit pas un préjudice basé sur un renseignement qui est inexact ou désuet à son égard. Des mesures raisonnables doivent être prises pour que les Renseignements personnels soient effacés ou rectifiés en temps opportun.

Conservation et anonymisation

Les Renseignements personnels ne doivent être conservés que pour la durée nécessaire à la réalisation des fins pour lesquelles ils ont été recueillis. Lorsque ces fins ont été accomplies, la Société doit détruire les Renseignements personnels. La Société peut également Anonymiser les Renseignements personnels,

selon les meilleures pratiques généralement reconnues et selon les critères et modalités déterminés par règlement, pour les utiliser à des fins sérieuses et légitimes seulement.

Sécurité et confidentialité

La Société a l'obligation de mettre en place des mesures de sécurité raisonnables propres à assurer la protection des Renseignements personnels qu'elle détient, utilise, communique, conserve ou détruit, contre la perte, le vol ou tout accès, communication, copie, utilisation, Traitement, modification ou destruction non autorisé ou abusif.

Ces mesures de sécurité doivent tenir compte notamment du degré de sensibilité des Renseignements personnels visés, de la finalité de leur utilisation, de leur quantité, de leur répartition, de leur méthode de conservation, de leur support et de leur format ainsi que des risques liés au respect de la vie privée.

Des mesures de sécurité adéquates devraient comprendre plusieurs couches de sécurité qui incluent, sans s'y limiter, des moyens techniques, matériels, organisationnels et administratifs.

5. Intégration de la protection des Renseignements personnels aux activités commerciales

Pour pouvoir se conformer aux principes généraux énoncés ci-dessus, la Société doit intégrer les pratiques décrites ci-dessous dans ses opérations et activités commerciales.

Notification aux personnes concernées

(Voir l'article 6 ci-dessous.)

Choix et consentement de la personne concernée

(Voir l'article 6 ci-dessous.)

Collecte de Renseignements personnels

Si des Renseignements personnels sont recueillis auprès de tiers, le Responsable de la protection des renseignements personnels doit s'assurer que la collecte est autorisée par la loi et qu'elle respecte les politiques et pratiques de la Société à ce sujet.

Pour ce faire, le Responsable de la protection des renseignements personnels réalise une cartographie des Activités de traitement et une analyse des Renseignements personnels qui sont collectés ainsi que leur destination. Selon le résultat de cette analyse, il décide de mener une ÉFVP et prépare, le cas échéant, un Formulaire de consentement de la personne concernée qui sera disponible au moment de la collecte.

Utilisation, conservation et destruction

Les objectifs, les méthodes, la période de conservation et les limites de stockage des Renseignements personnels doivent être conformes aux informations contenues dans la Politique de confidentialité de la Société et dans la Politique sur la gestion intégrée des documents et la sécurité de l'information.

La Société doit maintenir l'exactitude, l'intégrité, la confidentialité et la pertinence des Renseignements personnels en fonction de la finalité du Traitement.

Des mécanismes de sécurité raisonnables et adéquats doivent être utilisés pour empêcher le vol, l'utilisation abusive ou frauduleuse des Renseignements personnels et prévenir les Incidents de confidentialité.

Le Responsable de la protection des renseignements personnels est responsable du respect des exigences énumérées dans la présente section.

Pour ce faire, le Responsable de la protection des renseignements personnels doit procéder à une vérification des Renseignements personnels collectés et traité et construire un Registre des Renseignements personnels décrivant les renseignements utilisés au sein des documents produits par la Société, les fins pour lesquels ces renseignements ont été produits, les délais de conservation de ces documents et des renseignements qu'ils contiennent et les droits d'accès relatifs à chacun de ces documents.

Divulgarion à des tiers

Avant de transférer des Renseignements personnels à un fournisseur de services ou un partenaire commercial, le Responsable de la protection des renseignements personnels doit, à chaque fois, conclure un contrat écrit avec ce tiers, comme l'Entente relative à la sécurité de l'information concernant le Traitement des Renseignements personnels par un fournisseur de services, lequel doit prévoir au minimum :

- ! Une description des mesures prises par le fournisseur de services pour assurer la protection du caractère confidentiel des Renseignements personnels communiqués (ex. une description des mesures de sécurité);
- ! Une obligation pour le fournisseur de services de n'utiliser les Renseignements personnels qu'aux fins de la prestation des services et de ne pas conserver ces renseignements après l'expiration du contrat; et
- ! Une obligation pour le fournisseur de services d'informer sans délai le Responsable de la protection des renseignements personnels de toute violation ou tentative de violation d'une obligation relative à la confidentialité des renseignements et de permettre au responsable de la protection des Renseignements personnels d'effectuer toute vérification relative aux exigences de confidentialité.

À cette fin, le « **Questionnaire de conformité à l'attention des sous-traitants** » doit être utilisé. Une fois le formulaire rempli et retourné à l'attention du Responsable de la protection des renseignements personnels, ce dernier, avec le Comité de gouvernance, analyse les risques relatifs à la divulgation de Renseignements personnels. Sur la base de cette analyse, le Comité de gouvernance et le Responsable de la protection des renseignements personnels doivent entreprendre des discussions avec le

fournisseur de services afin qu'il implante au sein de son entreprise un programme de gouvernance qui respectera le Programme de gouvernance en place au sein de la Société et il devra s'engager à conclure une Entente relative à la sécurité de l'information.

Divulgence dans le cadre d'une transaction commerciale

Si la divulgation de Renseignements personnels est nécessaire dans le cadre d'une transaction commerciale, le Responsable de la protection des renseignements personnels doit, à chaque fois, conclure une entente écrite avec les parties qui prévoit notamment que la partie recevant communication des Renseignements personnels s'engage à :

- ! N'utiliser ces renseignements qu'aux seules fins de la conclusion de la transaction;
- ! Ne pas communiquer ces renseignements sans avoir obtenu le consentement des individus concernés;
- ! Prendre les mesures nécessaires pour assurer la protection du caractère confidentiel de ces Renseignements personnels; et
- ! Détruire ces Renseignements personnels si la transaction n'est pas conclue ou si leur utilisation n'est plus nécessaire aux fins de sa conclusion.

À cette fin, le ou les cocontractants doivent conclure avec la Société un engagement de confidentialité.

Transfert à l'extérieur du Québec

Le Responsable de la protection des renseignements personnels doit effectuer une Évaluation des facteurs relatifs à la vie privée avant de communiquer des Renseignements personnels à l'extérieur du Québec afin de déterminer si les Renseignements personnels bénéficieront d'une protection adéquate et suffisante au regard notamment des principes de protection des renseignements personnels généralement reconnus. Cette ÉFVP doit tenir compte de:

- ! La sensibilité du renseignement;
- ! La finalité de son utilisation;
- ! Les mesures de protection dont il bénéficierait;
- ! Le régime juridique applicable de la juridiction (ex. : pays, province, État) visée par la communication, notamment eu égard à son degré d'équivalence par rapport aux principes prévalant au Québec en matière de protection des Renseignements personnels.

Droit d'accès et rectification

La Société doit fournir aux personnes concernées qui en font la demande un accès gratuit (ou à un prix modique) à leurs Renseignements personnels et leur accorder la possibilité de les corriger, de les mettre à jour, de les rectifier ou de les effacer s'ils ne sont pas exhaustifs ou exacts, sous réserve des exceptions prévues par la loi. Le Responsable de la protection des renseignements personnels est chargé de veiller à ce que ces demandes soient traitées dans un délai d'un mois (30 jours), ne soient pas excessives et

n'affectent pas les droits à la vie privée de tiers. De plus, le Responsable de la protection des renseignements personnels doit également tenir et maintenir un registre de ces demandes. Lorsqu'une demande d'accès est refusée, le Responsable de la protection des renseignements personnels doit expliquer les raisons de ce refus à la personne concernée.

La procédure et les modalités du droit d'accès sont détaillées dans le document intitulé : « **Procédure de demande d'accès** ».

Droit à la portabilité

Une personne peut demander que les Renseignements personnels recueillis à son sujet soient communiqués ou transférés à une autre organisation qu'elle désigne dans un format technologique et couramment utilisé. Ceci exclut les renseignements créés ou inférés par la Société à partir de l'analyse des Renseignements personnels de la personne concernée. La Société n'est pas tenue de détruire les Renseignements personnels qu'elle détient après avoir traité une demande de portabilité.

Droit à la désindexation

Les personnes concernées peuvent demander à la Société, sous réserve de certaines conditions, de cesser de diffuser leurs Renseignements personnels et de désindexer tout hyperlien rattaché à leur nom qui donne accès à ces Renseignements personnels si cette diffusion contrevient à la loi ou à une ordonnance judiciaire. Le Responsable de la protection des renseignements personnels doit prendre les mesures nécessaires pour respecter ce droit à la désindexation et informer les tiers qui utilisent ou traitent ces Renseignements personnels afin de se conformer à la demande.

6. Lignes directrices pour un Traitement équitable

Les Renseignements personnels ne doivent être recueillis, utilisés, communiqués, conservés ou détruits que lorsque le Responsable de la protection des renseignements personnels l'autorise explicitement.

La Société doit procéder à une ÉFVP pour tout projet d'acquisition, de développement et de refonte d'un système d'information ou de prestation électronique de services impliquant la collecte, l'utilisation, la communication, la conservation ou la destruction de renseignements personnels. Dans chaque cas, le Responsable de la protection des renseignements personnels doit décider d'effectuer ou non une ÉFVP conformément au document intitulé « **Lignes directrices dans le cadre des évaluations des facteurs relatifs à la vie privée** ».

Droit d'être informé des personnes concernées

Avant de recueillir ou au moment de recueillir des Renseignements personnels, le Responsable de la protection des renseignements personnels doit communiquer aux personnes concernées les informations minimales suivantes :

- ! Les fins légitimes auxquelles ces renseignements sont recueillis;
- ! Les moyens par lesquels les renseignements sont recueillis;
- ! Les droits d'accès et de rectification prévus par la loi;

- ! Le droit pour la personne concernée de retirer son consentement à la communication ou à l'utilisation de ses renseignements en tout temps;
- ! Le nom du tiers pour qui la collecte est faite, le cas échéant;
- ! La possibilité que les renseignements soient communiqués à l'extérieur du Québec, le cas échéant;
- ! La possibilité que les renseignements soient communiqués à des fournisseurs de services, incluant des sociétés affiliées, le cas échéant, ou à d'autres tiers similaires;
- ! La durée de conservation de ces renseignements;
- ! Les coordonnées du Responsable de la protection des renseignements personnels.

Ces informations sont fournies par le biais d'une politique ou d'un avis de confidentialité. Lorsqu'il existe plusieurs activités de Traitement au sein de la Société, celle-ci doit élaborer différents avis ou politiques distincts selon l'activité de Traitement et les catégories de Renseignements personnels recueillis en cause. Le Responsable de la protection des renseignements personnels est responsable de créer et de maintenir un registre des avis de confidentialité (voir le Registre des avis de confidentialité).

Lorsque des renseignements personnels sont transférés à l'extérieur du Québec conformément à la « **Politique de transfert transfrontalier des données** », la politique de confidentialité doit le refléter et indiquer clairement où et à quelle entité les Renseignements personnels sont transférés.

Lorsque des Renseignements personnels sensibles sont recueillis, le Responsable de la protection des renseignements personnels doit s'assurer que la politique de confidentialité indique explicitement la raison pour laquelle ces Renseignements personnels sensibles sont recueillis.

Obtenir les consentements

Lorsque le Traitement est fondé sur le consentement de la personne concernée, le Responsable de la protection des renseignements personnels est tenu de conserver une preuve que le consentement a été valablement obtenu. Le Responsable de la protection des renseignements personnels doit également informer les personnes concernées de leur droit de retirer leur consentement et veiller à ce que leur consentement (lorsque celui-ci est utilisé comme fondement légitime du Traitement) puisse être retiré en tout temps.

Lorsque la collecte de Renseignements personnels concerne un enfant de moins de 14 ans, le Responsable de la protection des renseignements personnels doit s'assurer que le consentement de l'autorité parentale ou du tuteur du mineur a été obtenu avant la collecte à l'aide du **Formulaire de consentement parental**.

Les Renseignements personnels ne doivent être traités qu'aux fins légitimes et nécessaires pour lesquelles ils ont été initialement recueillis. Si la Société souhaite utiliser les Renseignements personnels recueillis à une autre fin, elle doit demander le consentement des personnes concernées par écrit, de manière claire et concise. Toute demande de ce type doit inclure les éléments suivants :

- ! La fin initiale pour laquelle les renseignements ont été recueillis;
- ! La ou les nouvelles fin(s) visée(s) (ou les fins secondaires);
- ! La raison du changement de fin(s).

Le Responsable de la protection des renseignements personnels est responsable du respect des règles énoncées au présent paragraphe.

7. Organisation et gouvernance

La responsabilité de garantir la protection et le Traitement adéquat des Renseignements personnels incombe à la Société et à toute personne qui travaille avec ou pour le compte de la Société et qui a accès aux Renseignements personnels de la Société.

Les principales responsabilités en matière de gouvernance et de gestion des Renseignements personnels relèvent des rôles organisationnels suivants :

- Le **Comité de gouvernance** est responsable des tâches suivantes :
 - Prendre des décisions et approuver les stratégies générales de la Société en matière de protection des Renseignements personnels;
 - Approuver toute déclaration publique touchant à la protection des Renseignements personnels jointe à des communications telles que des courriels, des lettres et des avis publics;
 - Répondre à toute demande de renseignements sur la protection des Renseignements personnels provenant de journalistes ou d'organes de presse;
 - Si nécessaire, travailler avec le Responsable de la protection des renseignements personnels pour s'assurer que les initiatives de marketing respectent les principes de protection des Renseignements personnels;
 - S'assurer que tous les systèmes, services et équipements informatiques utilisés par la Société pour le stockage des données et des Renseignements personnels répondent à des normes de sécurité acceptables;
 - Effectuer des évaluations, des analyses et des mises à jour régulières pour s'assurer que le matériel, les technologies et les logiciels de sécurité fonctionnent correctement;
 - S'assurer que la Société se réserve le droit d'auditer les fournisseurs de services;
 - Déterminer et surveiller les droits d'accès aux documents et autres données de la Société;
 - Sensibiliser les fournisseurs de services et autres tiers qui travaillent avec ou pour le compte de la Société à la protection des Renseignements personnels;
 - Offrir aux employés de la formation continue sur les Incidents de confidentialité et les techniques de cyberattaque afin de les tenir à jour et d'éviter que les mesures de contrôle informatiques ne deviennent inutiles;
 - Participer à l'élaboration de la documentation et l'implantation des politiques et procédures développées dans le cadre du Programme de gouvernance de l'information et notamment la Politique sur la gestion intégrée des documents et de sécurité de l'information;
 - Recevoir, enregistrer, classer et voir à la destruction des documents et des Renseignements personnels à la fin de leur délai de rétention;
 - Participer à la mise à jour des outils de classification, du calendrier de conservation et tout autre outil similaire;

- Offrir aux employés ayant un accès aux systèmes essentiels de la Société une formation de base sur les bonnes pratiques en matière de gestion documentaire et des Renseignements personnels;
 - S'assurer que les Renseignements personnels des employés soient traités à des fins légitimes et nécessaires par l'employeur;
 - Gérer les transferts de Renseignements personnels aux fournisseurs de services et autres tiers qui travaillent avec ou pour le compte de la Société;
 - Transmettre aux fournisseurs de services et autres tiers qui travaillent avec ou pour le compte de la Société la documentation pertinente en matière de protection des Renseignements personnels
- **Le Responsable de la protection des Renseignements personnels** est responsable des tâches suivantes, tel que défini dans le document intitulé « Description du poste de Responsable à la protection des renseignements personnels » :
- Gérer et mettre en œuvre le Programme de gouvernance de l'information;
 - Développer et promouvoir les politiques et les pratiques de la Société en matière de protection des Renseignements personnels;
 - Surveiller et analyser les lois sur la vie privée applicables ainsi que les changements qui sont envisagés ou apportés par le législateur;
 - Élaborer et maintenir à jour les exigences de conformité que la Société doit respecter et aider celle-ci à atteindre ses objectifs en matière de protection des Renseignements personnels;

8. Signalement et réponse aux Incidents de confidentialité

La Société doit aviser la Commission d'accès à l'information et les personnes concernées de tout Incident de confidentialité qui présente un risque de préjudice sérieux compte tenu de la sensibilité des renseignements concernés, des conséquences appréhendées de leur utilisation et la probabilité qu'ils soient utilisés à des fins préjudiciables. Le signalement des Incidents de confidentialité doit être effectué sans délai excessif et, si possible, dans les 72 heures de l'incident, conformément à la Procédure de réponse et de notification en cas d'Incident de confidentialité.

9. Audit

Le Responsable à la protection des Renseignements personnels est chargé d'auditer la manière dont la Société met en œuvre la présente Politique.

10. Sanctions

Toute personne qui enfreint cette Politique fera l'objet d'une sanction disciplinaire et pourra également être soumise à des poursuites civiles ou pénales si sa conduite enfreint les lois ou les règlements applicables.

11. Conflits

La présente Politique vise à se conformer aux lois et règlements et aux ententes d'affaires qui s'appliquent à la Société dans le cadre de ses opérations et activités commerciales. En cas de conflit entre la présente Politique et les lois et règlements applicables, ces derniers prévaudront.

12. Gestion documentaire

Nom du registre	Lieu de conservation	Personne responsable de la conservation	Mesures de protection en place	Période de rétention
Registre des consentements de la personne concernée	Logiciel Para-Maître	Responsable à la protection des Renseignements personnels	Seules les personnes autorisées peuvent accéder au registre et aux formulaires	10 ans
Registre des Activités de traitement	Logiciel Para-Maître	Responsable à la protection des Renseignements personnels	Seules les personnes autorisées peuvent accéder au registre	Permanent
Registre des droits de la personne concernée	Logiciel Para-Maître	Responsable à la protection des Renseignements personnels	Seules les personnes autorisées peuvent accéder au registre	Permanent
Registre des Renseignements personnels	Logiciel Para-Maître	Responsable à la protection des Renseignements personnels	Seules les personnes autorisées peuvent accéder au registre	Permanent
Registre des communications	Logiciel Para-Maître	Responsable à la protection des Renseignements personnels	Seules les personnes autorisées peuvent accéder	Permanent

			au registre	
Registre des avis de confidentialité	Logiciel Para-Maître	Responsable à la protection des Renseignements personnels	Seules les personnes autorisées peuvent accéder au registre	Permanent

13. Validité

Ce document entre en vigueur à compter du 21 mai 2024.

Le propriétaire du présent document est le Responsable de la protection des renseignements personnels, qui doit le vérifier et le mettre à jour au moins une fois par an.

Directrice générale
Réseau Notarial Plus

Caroline Lamoureux-Larochelle