



POLITIQUE CADRE DE PROTECTION DES RENSEIGNEMENTS PERSONNELS

| | |
|----------------------------------|---|
| <i>Code:</i> | |
| <i>Version:</i> | <i>1.0</i> |
| <i>Date de version</i> | <i>2024-11-04</i> |
| <i>Créé</i> | <i>Therrien Couture Jolicœur S.E.N.C.R.L.</i> |
| <i>Approuvé par</i> | |
| <i>Niveau de confidentialité</i> | <i>Confidentiel</i> |

Historique des modifications

| <i>Date</i> | <i>Version</i> | <i>Auteur(s)</i> | <i>Description des modifications</i> |
|--------------------|-----------------------|-------------------------|---|
| <i>2021.01.19</i> | <i>1.0</i> | <i>TCJ</i> | <i>Création du document de base</i> |
| <i>2024-04-11</i> | <i>2.0</i> | <i>Odette Mercier</i> | <i>Implantation de la politique et ajout des informations de l'organisation</i> |
| | | | |
| | | | |
| | | | |

Table des matières

| | |
|--|-----------|
| 1. OBJET ET PORTÉE DE LA POLITIQUE..... | 4 |
| 2. DOCUMENTS DE RÉFÉRENCE..... | 4 |
| 2.1. LÉGISLATION PERTINENTE..... | 4 |
| 3. DÉFINITIONS..... | 5 |
| 4. PRINCIPES GÉNÉRAUX..... | 6 |
| 4.1. RESPONSABILISATION ET GOUVERNANCE..... | 6 |
| 4.2. CONSENTEMENT..... | 7 |
| 4.3. ÉQUITÉ ET LÉGALITÉ..... | 7 |
| 4.4. TRANSPARENCE..... | 7 |
| 4.5. DÉTERMINER LES FINS DE LA COLLECTE ET DE L'UTILISATION..... | 8 |
| 4.6. EXACTITUDE ET RECTIFICATION..... | 8 |
| 4.7. CONSERVATION ET ANONYMISATION..... | 9 |
| 4.8. SÉCURITÉ ET CONFIDENTIALITÉ..... | 9 |
| 5. FINALITÉS DE TRAITEMENT LÉGITIMES DES RENSEIGNEMENTS CONCERNANT LES EMPLOYÉS | 9 |
| 5.1. GESTION DES RESSOURCES HUMAINES..... | 9 |
| 5.2. AUTRES ACTIVITÉS..... | 10 |
| 5.3. CONFORMITÉ AVEC LA LOI..... | 10 |
| 6. INTÉGRATION DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS AUX ACTIVITÉS COMMERCIALES..... | 10 |
| 6.1. COLLECTE DE RENSEIGNEMENTS PERSONNELS..... | 10 |
| 6.2. COLLECTE DE RENSEIGNEMENTS PERSONNELS DES EMPLOYÉS..... | 11 |
| 6.3. UTILISATION, CONSERVATION ET DESTRUCTION..... | 11 |
| 6.4. UTILISATION, CONSERVATION ET DESTRUCTION DES RENSEIGNEMENTS PERSONNELS DES EMPLOYÉS..... | 11 |
| 6.5. DIVULGATION À DES TIERS..... | 12 |
| 6.6. DIVULGATION DANS LE CADRE D'UNE TRANSACTION COMMERCIALE..... | 13 |
| 6.7. TRANSFERT À L'EXTÉRIEUR DU QUÉBEC..... | 13 |
| 6.8. DROIT D'ACCÈS ET RECTIFICATION..... | 13 |
| 6.9. DROIT À LA PORTABILITÉ..... | 14 |
| 6.10. DROIT À LA DÉSINDEXATION (DROIT À L'OUBLI)..... | 15 |
| 7. ORGANISATION ET GOUVERNANCE..... | 15 |
| 8. SIGNALEMENT D'INCIDENTS DE CONFIDENTIALITÉ ET RÉPONSE AUX PLAINTES.... | 16 |
| 9. AUDIT..... | 16 |
| 10. SANCTIONS..... | 16 |
| 11. CONFLITS..... | 16 |
| 12. AUTRES MEMBRES DU PERSONNEL..... | 16 |
| 13. GESTION DOCUMENTAIRE..... | 17 |
| 14. VALIDITÉ..... | 18 |

1. Objet et portée de la Politique

*La protection des Renseignements personnels est au cœur des préoccupations de **Le Groupe Jacques** (l' « **Organisation** »). C'est pourquoi nous nous engageons à respecter la vie privée de chacun conformément aux lois, règlements et normes applicables au Québec en matière de protection des Renseignements personnels.*

*Dans la présente politique de protection des Renseignements personnels (la « **Politique** »), vous constaterez que nous adhérons à des principes et à des pratiques que nous mettons en œuvre lorsque nous recueillons, utilisons, communiquons, conservons, ou détruisons les Renseignements personnels de nos clients, fournisseurs, partenaires commerciaux, employés et autres personnes en relation avec nous, dans le cadre de nos activités. Cette Politique présente également les responsabilités qui incombent au Responsable de la protection des Renseignements personnels et vous indique la structure de gouvernance adoptée grâce à la création de divers comités.*

La Politique s'applique à tous ses employés, comités, fournisseurs de services, partenaires commerciaux et autres contractants qui travaillent pour le compte ou avec l'Organisation ainsi qu'aux personnes visées par l'article 12 des présentes.

2. Documents de référence

2.1. Législation pertinente

- *Loi sur la protection des renseignements personnels dans le secteur privé, CQLR c P-39.1 (la « **Loi sur le secteur privé** »);*
- *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels, SQ 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, LC 2010, ch 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 québécoises sur la protection de la vie privée** »)*

3. Définitions

Voici quelques définitions pour vous aider à mieux comprendre :

Activité de traitement ou Traitement : toute opération effectuée sur ou avec des renseignements personnels au cours de leur cycle de vie, que ce soit ou non par des moyens automatisés, en débutant par la collecte, puis l'utilisation, la communication, la conservation et finalement la destruction ainsi que toutes les activités en lien avec ces opérations.

Ajout de bruit : Cette méthode implique l'ajout intentionnel d'erreurs ou de données aléatoires aux enregistrements. Cela peut rendre plus difficile la réidentification des individus tout en préservant la structure globale des données.

Anonymiser : poser une action sur un renseignement personnel concernant un individu de sorte qu'on ne puisse plus jamais, et ce de façon irréversible, identifier directement ou indirectement cette personne.

Dépersonnaliser : supprimer, remplacer ou retirer tous les renseignements qui permettent l'identification directe de la personne concernée. S'il y a remplacement des noms et identifiants évidents, cela permettra de faire en sorte qu'on ne puisse plus identifier directement la personne concernée. Cela peut se faire grâce à des techniques telles que la troncation, l'ajout de bruit, l'utilisation d'outils de chiffrement, la réduction du niveau de granularité des informations ou une combinaison de ces techniques et/ou l'utilisation de techniques additionnelles.

Évaluation des facteurs relatifs à la vie privée ou ÉFVP : démarche conçue pour évaluer les Activités de traitement et leur nécessité, qui sont proportionnelles à la fin recherchée et s'assurer que le Traitement ne risque pas de porter atteinte à la vie privée d'un individu.

Incident de confidentialité : tout accès non autorisé par la loi à un renseignement personnel, à son utilisation ou à sa communication, de même que sa perte ou toute autre forme d'atteinte à sa protection ou à son caractère confidentiel.

Pseudonymisation : processus de sécurité réversible qui consiste à remplacer des renseignements facilement attribuables à une personne (par exemple, son nom et son prénom) ou des éléments qui permettent de la distinguer des autres (personne de plus de 100 ans) par des renseignements uniques de sorte que les données originales ne soient plus directement liées à une personne. Les identifiants directs sont remplacés par des alias et ils ne permettent qu'une identification indirecte de la personne concernée et ce, uniquement pas les personnes en possession de la clé d'association de l'alias au renseignement personnel (un alias ou un numéro de référence ou un code).

Renseignements personnels : désigne tout renseignement qui concerne une personne physique et permet de l'identifier directement ou indirectement, 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 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). Cela inclut dans tous les cas, un Renseignement personnel sensible.

Renseignements personnels sensibles : renseignement personnel qui, par sa nature ou en raison du contexte de son utilisation ou de sa communication, suscite un haut degré d'attente raisonnable de protection de la part de la personne concernée (par exemple, des renseignements médicaux, biométriques, génétiques ou financiers, ou encore de renseignements sur la vie ou l'orientation sexuelle, les convictions religieuses ou philosophiques, l'appartenance syndicale ou bien l'origine ethnique).

Responsable de la protection des renseignements personnels : La personne désignée pour s'assurer de la protection de la vie privée au sein de l'Organisation (RPRP).

Troncation : La troncation consiste à raccourcir les données, par exemple en utilisant uniquement les trois premières lettres du nom d'un client plutôt que le nom complet.

Utilisation d'outils de chiffrement : Le chiffrement peut être utilisé pour rendre les données illisibles sans la clé de déchiffrement appropriée. Cependant, cela peut ne pas être suffisant pour l'anonymisation complète, car la réidentification reste possible si la clé est compromise.

4. Principes généraux

La Loi sur le secteur privé du Québec et la Loi 25 ainsi que certains contrats avec lesquels l'Organisation est liée nous obligent à nous conformer aux principes généraux suivants :

4.1. Responsabilisation et gouvernance

L'Organisation est responsable de la protection des Renseignements personnels qu'elle détient, utilise, communique, conserve ou détruit. C'est pourquoi elle :

- désigne un RPRP;
- établit et met en œuvre des politiques et des pratiques encadrant sa gouvernance à l'égard des Renseignements personnels;
- établit un processus de réponse aux demandes d'accès et de rectification qui lui sont transmises;
- publie sur son site Web son Programme de gouvernance de l'information;
- établit un processus de gestion des incidents de confidentialité; elle avisera d'ailleurs la Commission d'accès à l'information et les personnes concernées de tout Incident de confidentialité dans le cas où il peut en découler un préjudice sérieux pour ces dernières

4.2. Consentement

Les Renseignements personnels ne doivent être collectés et traités qu'aux fins légitimes et nécessaires pour lesquelles ils ont été initialement recueillis. Aussi, avant de recueillir, d'utiliser ou de communiquer des Renseignements personnels, l'Organisation doit obtenir un consentement valable de la part de la personne concernée. C'est pourquoi nous recueillons ce consentement de manière explicite, sous réserve de situations où le consentement peut être implicite en vertu de la loi. Il doit cependant être donné de manière expresse s'il concerne des Renseignements personnels sensibles.

Le consentement ne vaut que pour la durée nécessaire à la réalisation des fins pour lesquelles il a été demandé.

Pour utiliser les Renseignements personnels à une fin secondaire ou autre, il est nécessaire d'obtenir un consentement additionnel. Ce dernier sera énoncé ou rédigé de façon simple et claire et inclure :

- 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).*

Une preuve que le consentement a été valablement obtenu est conservée par l'Organisation.

Le RPRP est responsable du respect des règles concernant l'obtention du consentement de façon légale et appropriée.

4.3. Équité et légalité

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

C'est pourquoi nous formons et sensibilisons de façon récurrente nos employés à l'égard des politiques et des pratiques de gestion des Renseignements personnels de l'Organisation. Elles sont rédigées en termes simples et clairs pour en faciliter la compréhension et sont faciles d'accès pour nos employés comme pour nos clients.

4.4. Transparence

L'Organisation doit faire preuve de transparence et voir à informer ses résidents et ses employés des politiques et des pratiques de gestion des Renseignements.

C'est ainsi qu'avant de recueillir ou au moment de recueillir des Renseignements personnels, nous vous mentionnons les informations minimales suivantes :

- *Les fins légitimes auxquelles ces Renseignements sont recueillis;*
- *Les moyens par lesquels les Renseignements sont recueillis;*
- *Vos droits d'accès et de rectification prévus par la loi;*
- *Votre droit de retirer votre consentement à la communication ou à l'utilisation de ces 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.*
- *La possibilité que les renseignements soient communiqués à des fournisseurs de services, incluant des organisations affiliées, le cas échéant, ou à d'autres tiers similaires;*
- *La durée de conservation de ces renseignements (sur demande);*
- *Les coordonnées du RPRP.*

De plus, en tout temps et sur demande de votre part, nous vous communiquerons des informations additionnelles comprenant:

- *Les Renseignements personnels que vous nous avez communiqués;*
- *Les catégories de personnes qui ont accès à ces Renseignements personnels au sein de l'Organisation;*

4.5. 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 communiqués. Ces fins sont établies avant la collecte et l'utilisation des Renseignements personnels, qui ne doivent pas être effectuées d'une manière incompatible avec ces fins établies, sous réserve du consentement obtenu. L'Organisation doit faire preuve d'honnêteté et de transparence au sujet des raisons pour lesquelles elle recueille des Renseignements personnels et il est important que tous comprennent bien ce que nous en ferons.

4.6. Exactitude et rectification

Les Renseignements doivent être à jour et exacts au moment où nous les utilisons pour prendre une décision. Nous visons à sauvegarder l'intégrité de l'information, tant dans son fond que sa forme, et à nous assurer que personne ne subit de préjudice si un Renseignement devait être inexact ou désuet. Nous prenons des mesures raisonnables et adoptons les meilleures pratiques pour que les Renseignements personnels soient maintenus à jour et qu'ils soient ou rectifiés s'ils doivent l'être ou effacés lorsque devenus inutiles.

4.7. Conservation et anonymisation

Les Renseignements ne sont conservés que pour la durée nécessaire à la réalisation des fins pour lesquelles ils ont été recueillis. Lorsque ces fins sont accomplies, nous devons détruire les Renseignements personnels. L'Organisation peut également Anonymiser les Renseignements personnels, selon les meilleures pratiques généralement reconnues, pour utiliser les Renseignements anonymisés à des fins sérieuses et légitimes seulement.

Il est possible que certaines lois spécifient une période de conservation que l'Organisation sera tenue de respecter.

4.8. Sécurité et confidentialité

Nous avons l'obligation de mettre en place des mesures de sécurité raisonnables propres à assurer la protection des Renseignements personnels détenus, utilisés, communiqués, conservés contre la perte, le vol ou tout accès, communication, copie, utilisation, traitement, modification ou destruction non autorisé ou abusif.

Ces mesures de sécurité tiennent 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 qui comprennent plusieurs couches de sécurité incluant, sans s'y limiter, des moyens techniques, matériels, organisationnels et administratifs ont été implantées au sein de l'Organisation.

5. Finalités de Traitement légitimes des renseignements concernant les employés

L'Organisation peut utiliser les Renseignements personnels de ses employés pour des fins légitimes, dont certaines sont décrites ci-dessous :

5.1. Gestion des ressources humaines

Pour nous permettre de gérer les ressources humaines, notamment en ce qui concerne de nombreux processus : recrutement, exécution d'un contrat de travail, cessation d'emploi, gestion des performances, formation des employés, rémunération et avantages sociaux, services divers aux employés, santé et sécurité au travail, invalidité et processus de retour au travail, ainsi que toute autre activité de ressources humaines.

L'employé qui fournit des Renseignements personnels consent implicitement à leur collecte et à leur utilisation par l'Employeur. L'Organisation peut traiter les Renseignements personnels de ses employés sans renouveler ce consentement tant que l'employé est à son emploi, car à titre d'employeur, l'Organisation a une obligation légitime de recueillir les Renseignements personnels de ses employés pour gérer sainement et efficacement ses activités. Toutefois, les besoins d'information de l'Organisation doivent être compatibles au droit des employés à la protection de leurs Renseignements personnels.

5.2. *Autres activités*^[NB1]

Pour nous permettre de réaliser nos activités et opérations locatives et commerciales, telles que la gestion des actifs de l'Organisation, la prestation de services informatiques ou web, la sécurité de l'information, la réalisation d'audits et d'enquêtes internes, le respect des obligations de ses contrats commerciaux, obtenir des conseils juridiques ou commerciaux, la préparation de litiges juridiques, etc.

5.3. *Conformité avec la loi*

Pour nous permettre de nous conformer aux obligations légales et à toute autre fin requise par la loi, incluant celle de divulguer des Renseignements personnels des employés et résidents aux autorités fiscales compétentes.

6. *Intégration de la protection des Renseignements personnels aux activités commerciales*

En application principes généraux énoncés ci-dessus, l'Organisation intègre les pratiques décrites ci-dessous tout au long du cycle de vie des Renseignements personnels dans ses opérations et activités commerciales.

6.1. *Collecte de Renseignements personnels*

Lorsque nous collectons des Renseignements personnels, c'est d'abord directement auprès de la personne concernée nous les recueillons, après avoir mentionné l'information prévue à l'article 4.5.

Cependant, 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 l'Organisation à ce sujet.

En tout temps, nous limitons la collecte des Renseignements personnels à ce qui est nécessaire pour les fins déterminées qui ont été mentionnées.

6.2. Collecte de Renseignements personnels des employés

Lorsque nous recueillons des Renseignements personnels des employés, cette collecte doit se limiter aux Renseignements personnels qui sont strictement nécessaires à la réalisation des fins prévues telles que celles énoncées à l'article 4.5.

Si des Renseignements personnels d'un candidat à un emploi sont recueillis auprès de tiers, nous nous assurons que la collecte est effectuée par des moyens légitimes et légaux dans le respect des lois, des politiques et pratiques de l'Organisation.

6.3. Utilisation, conservation et destruction

Les objectifs, les méthodes, la période de conservation et les limites de stockage des Renseignements personnels sont conformes aux informations contenues dans la Politique sur la gestion intégrée des documents.

C'est le RPRP qui doit procéder à une vérification annuelle [NB2] des Renseignements personnels collectés et traités et construire un Registre des Renseignements personnels décrivant les renseignements utilisés au sein des documents produits par l'Organisation, les fins pour lesquelles ces renseignements ont été produits, les délais de conservation de ces documents et des renseignements qu'ils contiennent ainsi que les droits d'accès relatifs à chacun de ces documents.

Puisque nous devons maintenir l'exactitude, l'intégrité, la confidentialité et la pertinence des Renseignements personnels en fonction de la finalité du Traitement et de plus, ne les conserver que pour le temps dont nous en avons besoin à ces fins, nous avons mis en place des mécanismes de sécurité raisonnables et adéquats pour empêcher le vol, l'utilisation abusive ou frauduleuse des Renseignements personnels et prévenir les Incidents de confidentialité.

C'est pourquoi nous nous assurons également que les Renseignements personnels en notre possession ne sont ni détruits ni modifiés illégalement et nous nous engageons également à ne pas vendre ou fournir les Renseignements personnels à un tiers de manière illégale ou sans en obtenir l'autorisation. Nous effectuons des audits régulièrement pour nous en assurer.

6.4. Utilisation, conservation et destruction des Renseignements personnels des employés

Pour la presque totalité des Renseignements personnels des employés, y compris les dossiers relatifs à la paie et aux avantages sociaux, les dossiers personnels officiels et officieux, les enregistrements de navigation sur Internet, le courrier électronique et les pistes d'audit, les règles fondamentales suivantes sont respectées afin de maintenir un équilibre entre les droits de l'Organisation et ceux des employés :

- *Nous ne traitons les Renseignements personnels des employés qu'aux seules fins pour lesquelles ceux-ci ont été recueillis et ne conservons ces derniers que pour le temps dont nous en avons besoin, sauf si nous avons obtenu le consentement de l'employé concerné pour les utiliser à d'autres fins ou si nous devons, en vertu des lois applicables, utiliser ou communiquer les Renseignements personnels de l'employé à d'autres fins comme à la demande d'autorités de réglementation.*
- *Nous avons également mis en place des mesures de sécurité raisonnables propres à assurer la protection des renseignements personnels de nos employés contre la perte, le vol ou tout accès, communication, copie, utilisation, traitement, modification ou destruction non autorisé ou abusif. Ces mesures de sécurité, ici aussi, comprennent plusieurs couches de sécurité dont des moyens techniques, matériels, organisationnels et administratifs permettant d'assurer la gestion des risques, des incidents et la continuité des activités.*
- *Pour ces Renseignements personnels, nous nous assurons également de ne pas détruire ou modifier illégalement les Renseignements personnels et nous nous engageons à ne pas vendre ou fournir les Renseignements personnels des employés à un tiers de manière illégale ou sans autorisation.*

6.5. Divulgarion à des tiers

Avant de transférer des Renseignements personnels à un fournisseur de services ou un partenaire commercial, le RPRP 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. Certaines clauses doivent nécessairement se retrouver à ce contrat telles que :

- *La 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);*
- *L'engagement, par 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*
- *L'obligation, pour le fournisseur de services, de nous informer sans délai de toute violation ou tentative de violation de la confidentialité des renseignements afin de nous permettre d'effectuer toute enquête ou vérification relative à cette violation.*

*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 RPRP, il analyse avec le Comité de gouvernance des données les risques relatifs à la divulgation de Renseignements personnels. Sur la base de cette analyse, le Comité de gouvernance des données et le Responsable de la protection des renseignements personnels doivent s'assurer que le fournisseur de services implante au sein de son entreprise un programme de gouvernance qui respectera le Programme de gouvernance de l'Organisation et le tiers devra également s'engager à conclure une Entente relative à la sécurité de l'information.*

6.6. Divulcation nécessaire à des fins de sécurité

L'Organisation peut, le cas échéant, communiquer un renseignement qu'elle détient en vue de protéger une personne ou un groupe de personnes identifiable lorsque l'Organisation a des motifs raisonnables de croire qu'un risque de préjudice sérieux de mort ou de blessures graves (notamment toute blessure psychologique ou physique qui peut nuire de façon importante l'intégrité physique, le bien-être ou la santé de l'individu concerné) menace cette personne ou ce groupe.

L'Organisation peut également, le cas échéant, communiquer un renseignement à tout corps policier ainsi que le Directeur des poursuites criminelles et pénales lorsqu'elle a raison de croire qu'une infraction à la loi se produit ou pourrait se produire.

6.7. Divulcation dans le cadre d'une transaction commerciale

Si la divulgation de Renseignements personnels est nécessaire dans le cadre d'une transaction commerciale, le RPRP doit, à chaque fois, conclure une entente écrite avec les parties à la transaction 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.*

C'est pourquoi nous nous assurons d'obtenir un Engagement relatif à la sécurité de l'information de la part de contractants.

6.8. Transfert à l'extérieur du Québec

Si des Renseignements personnels sont communiqués à l'extérieur du Québec, une Évaluation des facteurs relatifs à la vie privée (ÉFVP) sera effectuée. Elle prendra en compte les éléments prévus à la loi pour nous assurer que les Renseignements bénéficieront d'une protection adéquate et suffisante chez le récipiendaire des Renseignements.

6.9. Droit d'accès et rectification

En tout temps, toute personne bénéficie d'un accès gratuit (ou à un prix modique pour obtenir des reproductions) à ses Renseignements personnels. Elle peut également faire corriger ou mettre à jour les renseignements inexacts, sous réserve des exceptions prévues par la loi. Ces demandes sont traitées dans un délai de 30 jours et sont inscrites au Registre des demandes d'accès et de rectifications. Si une demande d'accès est refusée, le RPRP y répond par écrit et explique les raisons de ce refus.

6.9.1. Le majeur inapte

Une personne liée à un majeur inapte peut également rectifier et accéder aux renseignements de santé concernant ce majeur. Elle doit notamment attester sous serment de son intention d'ouvrir ou réviser une tutelle, d'homologuer un mandat de protection ou la représentation temporaire du majeur inapte. Une évaluation préalable doit conclure à l'inaptitude de la personne concernée à prendre soin d'elle-même et à administrer ses biens ou à accomplir un acte déterminé.

6.9.2. Une personne décédée

Un(e) conjoint(e)¹, un parent et l'enfant [JD3] d'une personne décédée a le droit d'être informé de l'existence d'un renseignement relatif à la cause de son décès, et d'y avoir accès. Toutefois, si la personne a refusé l'accès à ce renseignement à la personne en question, l'accès ne peut être octroyé.

Les personnes suivantes ont le droit d'être informées de l'existence d'un renseignement concernant le défunt et d'y avoir accès à la condition que ce soit nécessaire à l'exercice de ses droits et obligations à ce titre :

- *L'héritier;*
- *Le successible;*
- *Le légataire particulier;*
- *Le liquidateur d'une succession;*
- *Une personne désignée à titre de bénéficiaire d'une assurance-vie ou d'une indemnité de décès.*

Une personne liée génétiquement au défunt peut également être informée de l'existence d'un renseignement concernant le défunt et d'y avoir accès à la condition que cela soit nécessaire pour vérifier l'existence d'une maladie génétique ou à caractère familial.[JD4]

6.10. Droit de restreindre et refuser l'accès

Toute personne peut demander que l'accès à ses renseignements de la santé et des services sociaux soit restreint ou refusé à un intervenant en particulier ou un groupe d'intervenants. Ce droit ne peut être outrepassé qu'en cas de risque à la vie ou l'intégrité physique de la personne concernée.

Toute personne peut également exiger la restriction d'accès à ses renseignements de la santé et des services sociaux. La restriction d'accès peut être applicable aux personnes et situations suivantes :

- *À son conjoint², ses ascendants et ses descendants s'il s'agit d'un renseignement relatif à la cause de son décès; et*

¹ Le terme « conjoint » tel que mentionné dans la loi, implique un(e) conjoint(e) avec qui la personne est marié(e) uniquement.

² Le terme « conjoint » tel que mentionné dans la loi, implique un(e) conjoint(e) avec qui la personne est marié(e) uniquement.

- A un chercheur si l'accès envisagé est à des fins de sollicitation en vue de sa participation à un projet de recherche.

6.11. Droit à la portabilité

Toute personne qui demande que les Renseignements personnels recueillis à son sujet soient communiqués ou transférés à une autre organisation désignée, dans un format technologique et couramment utilisé. Ceci exclut les renseignements créés ou inférés par l'Organisation à partir de l'analyse de vos Renseignements personnels. Après le transfert, nous ne sommes pas tenus de détruire les Renseignements personnels traités dans cette demande.

6.12. Droit à la désindexation (droit à l'oubli)

Toute personne peut, sous réserve de certaines conditions, nous demander de cesser de diffuser des Renseignements personnels la concernant ou de désindexer tout hyperlien rattaché à son nom qui donne accès à ces Renseignements personnels si cette diffusion lui cause un préjudice ou contrevient à la loi ou à une ordonnance judiciaire. Si ces Renseignements sont ainsi utilisés par un mandataire, nous verrons à lui demander de procéder de cesser de diffuser ou de procéder à la désindexation.

7. Organisation et gouvernance

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

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

Le **RPRP** est responsable des tâches suivantes:

- Gérer et mettre en œuvre le Programme de gouvernance de l'information;
- Développer et promouvoir les politiques et les pratiques de l'Organisation 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 l'Organisation doit respecter et aider celle-ci à atteindre ses objectifs en matière de protection des Renseignements personnels.

De plus, l'Organisation s'est dotée d'un Comité de gestion intégrée des documents, de sécurité et de gouvernance veillant à la bonne marche des opérations dans le respect de la confidentialité des Renseignements personnels. Ce comité a des tâches bien définies détaillées dans un document expliquant ces diverses tâches, accessible sur demande.

8. Signalement d'incidents de confidentialité et réponse aux plaintes

Toute personne physique dont les renseignements personnels sont concernés par un Incident de confidentialité réel ou appréhendé peut formuler une plainte au Responsable de la protection des renseignements personnels, laquelle sera traitée conformément à la Procédure de réponse et de notification en cas de plainte et/ou d'incidents de confidentialité.

Nous aviserons la Commission d'accès à l'information et toutes les personnes concernées après enquête, si un risque de préjudice sérieux est appréhendé, 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. Si les renseignements concernés concernent l'état de santé ou les services sociaux ou de santé octroyés aux personnes concernées, nous aviserons également le ministre de la Santé et des Services sociaux.

9. Audit

Le RPRP est chargé d'auditer la manière dont l'Organisation 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 l'Organisation 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. Autres membres du personnel

L'Organisation doit également respecter et mettre en application la présente Politique lorsqu'elle exerce une Activité de traitement des Renseignements personnels des autres membres de son personnel, ce qui comprend notamment: (i) les personnes qui postulent auprès de l'Organisation ou qui prennent part au processus de recrutement de l'Organisation (ii) les anciens employés de l'Organisation ainsi que (iii) les personnes non-employés qui travaillent dans les bureaux de l'Organisation, dont les travailleurs autonomes, consultants, bénévoles et stagiaires.

13. Gestion documentaire


| Nom du registre | Lieu de conservation | Personne responsable de la conservation | Mesures de protection en place | Période de rétention |
|---|-----------------------------|--|---|-----------------------------|
| <i>Registre 1.03 des renseignements personnels</i> | <i>Réseau sécurisé</i> | <i>RPRP</i> | <i>Seules les personnes autorisées peuvent accéder au registre et aux formulaires</i> | <i>Permanent</i> |
| <i>Registre 2.02 des plaintes et incidents de confidentialité</i> | <i>Réseau sécurisé</i> | <i>RPRP</i> | <i>Seules les personnes autorisées peuvent accéder au registre</i> | <i>Permanent</i> |
| <i>Registre 3.04 des demandes accès/rectification/retranchement</i> | <i>Réseau sécurisé</i> | <i>RPRP</i> | <i>Seules les personnes autorisées peuvent accéder au registre</i> | <i>Permanent</i> |
| <i>Registre 3.14 des consentements de la personne concernée Employés et Résidents</i> | <i>Réseau sécurisé</i> | <i>RPRP</i> | <i>Seules les personnes autorisées peuvent accéder au registre</i> | <i>Permanent</i> |
| <i>Registre 4.02 des transferts</i> | <i>Réseau sécurisé</i> | <i>RPRP</i> | <i>Seules les personnes autorisées peuvent accéder au registre</i> | <i>Permanent</i> |
| <i>Registre 5.07 des droits d'accès</i> | <i>Réseau sécurisé</i> | <i>RPRP</i> | <i>Seules les personnes autorisées peuvent accéder au registre</i> | <i>Permanent</i> |
| <i>Registre 6.10 des autorisations des sites Web, applications</i> | <i>Réseau sécurisé</i> | <i>RPRP</i> | <i>Seules les personnes autorisées peuvent accéder au registre</i> | <i>Permanent</i> |

14. Validité

*Ce document entre en vigueur à compter du **2024-11-04***

*Le propriétaire du présent document est **Le Groupe Jacques**, qui doit le vérifier et le mettre à jour au moins une fois par an.*

Le responsable de la protection des renseignements personnels
Marie-Claude Pelchat



Signature