POLITIQUE DE PROTECTION DES RENSEIGNEMENTS PERSONNELS

[Clinique Podiatrique GBL Inc.]

Code:	
Version:	1.0
Date de version	17-05-2023
Créé	Therrien Couture Joli-Cœur S.E.N.C.R.L.
Approuvé par	
Niveau de confidentialité	Confidentiel

Historique des modifications

Date	Version	Auteur(s)	Description des modifications
17-05-2023	1.0	TCJ	Création du document de base

Table des matières

1. Objet et portée de la Politique

[Clinique Podiatrique GBL] est engagée à respecter la vie privée de chacun conformément aux lois, règlements et normes applicables au Québec 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 l'Organisation adhère ainsi que les pratiques que nous mettons en œuvre lorsque nous recueillons, utilisons, communiquons, conservons et 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 l'Entreprise.

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 l'Organisation.

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** »)

2.2. Autres documents

- Politique de protection des renseignements personnels des employés;
- Politique sur la gestion intégré des documents et la sécurité de l'information;

- Description du poste de Responsable de la protection des renseignements personnels;
- Lignes directrices pour répertorier les activités de traitement des données;
- Formulaire de consentement de la personne concernée;
- Formulaire de retrait du consentement de la personne concernée;
- Lignes directrices dans le cadre des évaluations des facteurs relatifs à vie privée;
- Procédure de transfert transfrontalier des renseignements personnels;
- Procédure de demande d'accès;
- Formulaire de demande d'accès;
- Procédure de réponse et de notification en cas d'incident de confidentialité;
- Questionnaire de conformité des fournisseurs avec les Lois québécoises sur la protection de la vie privée;
- Entente sur la sécurité de l'information concernant le traitement des renseignements personnels par un fournisseur de services;
- Registre des politiques 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.

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 de données à caractère personnel.

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'autre 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 ;
- 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 ;
- 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 religieuses ou philosophiques, l'appartenance syndicale ou bien l'origine ethnique.

Responsable de la protection des renseignements personnels : désigne l'individu qui veille à assurer le respect et la mise en œuvre des Lois québécoises sur la protection de la vie privée au sein de l'Organisation.

4. Principes généraux

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

4.1. Responsabilisation et gouvernance

L'Organisation est responsable de la protection des Renseignements personnels qu'elle détient, utilise, traite, communique, conserve ou détruit. Elle doit notamment :

- désigner une personne chargée d'assurer le respect et la mise en œuvre des Lois québécoises 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 vigueurs;
- Aviser la Commission d'accès à l'information et les personnes concernées de tout Incident de confidentialité.

4.2. Consentement

Avant de recueillir, d'utiliser ou de communiquer des Renseignements personnels, l'Organisation 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.

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

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.

4.4. Transparence

L'Organisation 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, l'Organisation 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 collectées;
- Les Renseignements personnels recueillis auprès d'elle;
- Les catégories de personnes qui ont accès à ces Renseignements personnels au sein de l'Organisation;
- La durée de conservation de ces renseignements;
- Les coordonnées du Responsable de la protection des renseignements personnels.

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 recueillis. Ces fins doivent être établies avant la collecte et l'utilisation des Renseignements personnels. L'Organisation doit faire preuve d'honnêteté et de transparence au sujet des raisons pour lesquelles elles recueillent des Renseignements personnels.

4.6. Limitation de la collecte et de l'utilisation

L'Organisation 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.

4.7. Exactitude et rectification

L'Organisation 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 rectifiés ou effacés en temps opportun.

4.8. 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, l'Organisation doit détruire les Renseignements personnels. L'Organisation peut également Anonymiser les Renseignements personnels, selon les meilleures pratiques généralement reconnues, pour les utiliser 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.

4.9. Sécurité et confidentialité

L'Organisation 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, l'Organisation doit intégrer les pratiques décrites ci-dessous dans ses opérations et activités commerciales.

5.1. Notification aux personnes concernées

Veuillez-vous référer à l'article 6.1 ci-dessous.

5.2. Choix et consentement de la personne concernée

Veuillez-vous référer à l'article 6.2 ci-dessous.

5.3. Collecte de Renseignements personnels

La collecte des Renseignements personnels doit être faite directement auprès de la personne concernée. Cette dernière doit être informée des éléments mentionnés à l'article 6.1 de cette Politique au plus tard au moment de la collecte de leurs renseignements.

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.

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.

5.4. 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 l'Organisation et dans la Politique sur la gestion intégrée des documents et la sécurité de l'information.

L'Organisation 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 biannuelle des Renseignements personnels collectés et traité et construire un Registre des

Renseignements personnels décrivant les renseignements utilisés au sein des documents produits par l'Organisation, les fins pour lesquels 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.

5.5. Divulgation 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 analyse les risques relatifs à la divulgation de Renseignements personnels. Sur la base de cette analyse, le Responsable de la protection des renseignements personnels doit 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 l'Organisation et le tiers devra s'engager à conclure une Entente relative à la sécurité de l'information.

5.6. Divulgation 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 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.

À cette fin, le ou les cocontractants doivent conclure avec l'Organisation un Engagement de confidentialité.

5.7. 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.

5.8. Droit d'accès et rectification

L'Organisation doit fournir aux personnes concernées qui en font la demande un accès gratuit (ou à un prix modique pour obtenir des reproductions) 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 de 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 répondre par écrit et 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** ».

5.9. 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 l'Organisation à partir de l'analyse des Renseignements personnels de la personne concernée. L'Organisation n'est pas tenue de détruire les Renseignements personnels qu'elle détient après avoir traité une demande de portabilité.

5.10. Droit à la désindexation (Droit à l'oubli)

Les personnes concernées peuvent demander à l'Organisation, 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 leur cause un préjudice ou 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.

L'Organisation 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 vie privée** ».

6.1. 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 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 organisations 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, lequel est accessible via le site web de l'Organisation. Lorsque plusieurs Activités de traitement sont effectuées avec ces Renseignements personnels, l'Organisation doit indiquer toutes les Activités de traitement dans cette politique ou avis et indiquer 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.

6.2. 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 l'Organisation 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 l'Organisation et à toute personne qui travaille avec ou pour le compte de l'Organisation et qui a accès aux Renseignements personnels de l'Organisation.

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

- 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 de 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 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.

8. Signalement et réponse aux incidents de confidentialité

L'Organisation 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 dans un délai raisonnable, conformément à la Procédure de réponse et de notification en cas d'incident de confidentialité.

9. Audit

Le Responsable de la protection des Renseignements personnels 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. 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	Règlements, Politiques, Directives et Procédures du système d'information	RPRP	Seules les personnes autorisées peuvent accéder au registre et aux formulaires	10 ans
Registre des Activités de traitement	Règlements, Politiques, Directives et Procédures du système d'information	RPRP	Seules les personnes autorisées peuvent accéder au registre	Permanent
Registre des droits de la personne concernée	Règlements, Politiques, Directives et Procédures du	RPRP	Seules les personnes autorisées	Permanent

	système d'information		peuvent accéder au registre	
Registre des Renseignements personnels	Règlements, Politiques, Directives et Procédures du système d'information	RPRP	Seules les personnes autorisées peuvent accéder au registre	Permanent
Registre des communications	Règlements, Politiques, Directives et Procédures du système d'information	RPRP	Seules les personnes autorisées peuvent accéder au registre	Permanent
Registre des avis de confidentialité	Règlements, Politiques, Directives et Procédures du système d'information	RPRP	Seules les personnes autorisées peuvent accéder au registre	Permanent

13. Validité

Ce document entre en vigueur à compter du **29-05-2023**.

Le propriétaire du présent document est **Guillaume Buithieu Legault** qui doit le vérifier et le mettre à jour au moins une fois par an.

[Clinique GBL Inc.]

_____

Par : Guillaume Buithieu Legault, propriétaire.