Loi 25 - Guide d'accompagnement

Protection des renseignements personnels

2024

Document préparé par Ostéopathie Québec
et la Fédération des kinésiologues du Québec
en collaboration avec Me Cynthia Chassigneux
(CHX Avocat inc.).

TABLE DES MATIÈRES

Objet du Guide d'accompagnement

Le Guide d'accompagnement a pour but de présenter aux membres d'Ostéopathie Québec le cadre juridique applicable au Québec en matière de protection des renseignements personnels à la lumière des modifications qui entrées en vigueur en septembre 2022 et 2023.

Ces modifications s'appliquent :

- aux ministères et organismes publics assujettis à la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (RLRQ, c. A-2.1, la « **Loi sur l'accès** »), incluant les établissements de santé ou de services sociaux, les organismes scolaires ou encore les ordres professionnels en ce qui concerne les documents détenus dans le cadre de l'exercice de la profession ;
- aux personnes qui recueillent, détiennent, utilisent ou communiquent à des tiers des renseignements personnels à l'occasion de l'exploitation d'une entreprise, incluant les entreprises individuelles exploitées par une personne physique (i.e. travailleur autonome), les sociétés de personnes (i.e. SENC, SENCRL, SEC), les sociétés par actions, les organismes sans but lucratif (« **OSBL** »), les associations ou encore les coopératives. Ces personnes sont assujetties à la *Loi sur la protection des renseignements personnels dans le secteur privé* (RLRQ, c. P-39.1, la « **LPRPSP** »).

À qui s'adresse le Guide d'accompagnement

Le Guide d'accompagnement s'adresse aux membres d'Ostéopathie Québec qui exploitent une entreprise et aux travailleurs autonomes, considérés comme des entreprises individuelles au sens de la Loi sur le secteur privé.

Modernisation du cadre juridique applicable à la protection des renseignements personnels

La *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels* (LQ 2021, c. 25, la « **Loi 25** »), adoptée le 21 septembre 2021 par l'Assemblée nationale du Québec, vient modifier, mais aussi ajouter plusieurs dispositions au régime juridique applicable au Québec en matière de protection des renseignements personnels.

Cette modernisation entre en vigueur selon le calendrier suivant :

22/09/2022	• **Responsabilité / Responsable** de la protection des renseignements personnels • Déclaration des **incidents de confidentialité** • Communication à des fins d'**étude**, de **recherche** ou de **production de statistiques /** À des **fins de transaction commerciale** • **Biométrie**
22/09/2023	• Règles encadrant la **gouvernance** • Renseignements personnels + sensibles, dépersonnalisés, anonymisés • Évaluation des facteurs relatifs à la vie privée (**EFVP**) • **Politique de confidentialité / Consentement** - Information • **Paramètre de confidentialité /** Fonction permettant d'**identifier**, de **localiser** ou d'effectuer un **profilage /** Décision fondée exclusivement sur un **traitement automatisé** • **Destruction / Anonymisation /** Cessation de diffusion - Désindexation • **Amendes - Sanctions administratives pécuniaires - Dommages-Intérêts**
22/09/2024	• Droit à la **portabilité**

Renseignement personnel

Un renseignement personnel est un renseignement qui **concerne une personne physique** (par ex. client, patient, bénéficiaire, employé, bénévole, stagiaire, fournisseur de services) et **permet, directement ou indirectement, de l'identifier**.

Cette définition vise entre autres :

- Nom, prénom, adresse postale, téléphone (maison, cellulaire);
- Adresse courriel;
- Date de naissance, âge;
- État civil;
- Nationalité;
- Antécédents médicaux, scolaires, professionnels, financiers;
- Numéro d'assurance sociale, d'assurance maladie, de permis de conduire;
- Etc.

Note : Depuis le 22 septembre 2023, les renseignements relatifs au nom, titre, fonction, adresse (postale et électronique) et numéro de téléphone **du lieu de travail** d'une personne seront considérés comme des renseignements personnels à caractère public.

Depuis le **22 septembre 2023**, sont également en vigueur les définitions suivantes :

- **Renseignement personnel sensible** : sont sensibles les renseignements personnels qui, **par leur nature**, notamment médicale, biométrique ou autrement intime, **ou en raison du contexte** de leur utilisation et communication, **suscitent un haut degré d'attente raisonnable en matière de vie privée**.

  Les membres d'Ostéopathie Québec qui entendent utiliser un renseignement personnel sensible à des fins autres que celles pour lesquelles il a été collecté ou encore communiquer un tel renseignement doivent obtenir le consentement des personnes concernées, plus précisément un consentement manifesté de façon expresse.

- **Renseignement personnel dépersonnalisé** : un renseignement est dépersonnalisé lorsqu'il **ne permet plus d'identifier directement** la personne concernée.

  Attention, le fait de retirer le nom de la personne concernée, mais de conserver les autres renseignements ne permet pas de considérer que le renseignement est dépersonnalisé. De plus, les renseignements dépersonnalisés demeurent des renseignements personnels, car ils permettent d'identifier indirectement la personne concernée.

  Les membres d'Ostéopathie Québec qui entendent utiliser des renseignements personnels, sans le consentement de la personne concernée, à des fins d'étude, de recherche ou de production de statistiques peuvent le faire dans la mesure où ce renseignement est dépersonnalisé.

Ils doivent alors prendre les mesures raisonnables afin de limiter les risques que quiconque procède à l'identification d'une personne physique à partir de renseignements dépersonnalisés sous peine d'amende.

- **Renseignement anonymisé**: un renseignement est anonymisé lorsqu'il est, en tout temps, raisonnable de prévoir dans les circonstances qu'il **ne permet plus, de façon irréversible, d'identifier directement ou indirectement** la personne concernée.

  Lorsque les fins pour lesquelles un renseignement personnel a été recueilli ou utilisé sont accomplies, les membres d'Ostéopathie Québec doivent le détruire **ou l'anonymiser pour l'utiliser à des fins sérieuses et légitimes**, sous réserve d'un calendrier de conservation prévu par une loi.

  Si la décision est prise d'anonymiser les renseignements personnels au lieu de les détruire, il convient de s'assurer que cela est fait selon les meilleures pratiques généralement reconnues. Il convient également de s'assurer que personne ne procède ou tente de procéder à l'identification d'une personne physique à partir de renseignements anonymisés sous peine d'amende.

Mesures à prendre / Questions à se poser

- Faire un inventaire des renseignements personnels afin de déterminer la nature de ceux-ci, mais aussi leur support (papier, serveur, infonuagique, etc.), leur répartition (interne, externe), la durée de conservation.

Pour aller plus loin :

- COMMISSION D'ACCÈS À L'INFORMATION, Protection des renseignements personnels, distinguer anonymisation et dépersonnalisation
- GOUVERNEMENT DU QUÉBEC – *Projet de règlement sur l'anonymisation des renseignements personnels* – Gazette officielle – 20 décembre 2023

Responsabilité et Responsable de la protection des renseignements personnels

Depuis le **22 septembre 2022**, la Loi 25 reconnaît formellement que toute personne qui exploite une entreprise est « **responsable** de la protection des renseignements personnels qu'elle détient » et, ce que même si leur conservation est assurée par un tiers.

Cette obligation fait en sorte que les membres d'Ostéopathie Québec doivent être en mesure de démontrer, en tout temps, les mesures prises (en cours ou à venir) pour respecter leurs obligations en matière de protection des renseignements personnels.

Mesures à prendre / Questions à se poser

- Mettre en place un tableau de bord avec les actions à prendre / réalisées en indiquant les dates de réalisation ou à venir.

Pour assurer le respect et la mise en œuvre des exigences relatives à la protection des renseignements personnels, la Loi 25 prévoit que la personne ayant la plus haute autorité au sein d'une entreprise assume la fonction de **responsable de la protection des renseignements personnels**.

Toutefois, cette fonction peut être déléguée, par écrit, en tout ou en partie, à toute personne à l'interne ou à l'externe. La Loi 25 ne précise ni la forme, ni le contenu de cette délégation, ni le profil requis pour exercer cette fonction.

Les titres et coordonnées du responsable de la protection des renseignements personnels doivent être publiés sur le site Internet du membre d'Ostéopathie Québec ou être rendus accessibles par tout autre moyen (affiche, lettre d'information, contrat, politique de confidentialité).

Mesures à prendre / Questions à se poser

- Description des rôles et responsabilités du responsable de la protection des renseignements personnels, incluant notamment :
    - Assurer le respect et la mise en œuvre de la LPRPSP;
    - Approuver les politiques et pratiques encadrant la gouvernance des renseignements personnels;
    - Contribuer à l'évaluation des facteurs relatifs à la vie privée des projets d'acquisition, de développement et de refonte des systèmes d'information ou de prestation électronique de services impliquant des renseignements personnels;
    - Consigner toute communication faite à une personne ou à un organisme susceptible de diminuer les incidents de confidentialité;
    - Participer à l'évaluation du risque qu'un préjudice grave soit causé aux personnes dont les renseignements personnels sont visés par un incident de confidentialité;
    - Être informé sans délai d'un incident de confidentialité par un prestataire de service;
    - Procéder à toute vérification relative à la confidentialité des renseignements personnels chez un prestataire de service;
    - Répondre aux demandes d'accès, de rectification, de cessation de diffusion, de désindexation.
- Désigner le responsable de la protection des renseignements personnels :
    - Personne ayant la plus haute autorité ou délégation ?
        - Si délégation, prévoir un acte de délégation (voir modèle ci-joint)
- Titre et coordonnées à diffuser sur Internet ou par tout autre moyen.

Modèle : Résolution pour la délégation des fonctions de responsable de la protection des renseignements personnels

[Nom l'entité juridique]
(La « **Personne morale** »)

RÉSOLUTION du conseil d'administration de la Personne morale adoptée en date du xx-xx-xxxx

PROTECTION DES RENSEIGNEMENTS PERSONNELS

ATTENDU l'adoption de la *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels* (LQ 2021, c. 25, la « Loi 25 ») venant modifier la *Loi sur la protection des renseignements personnels dans le secteur privé* (RLRQ, c. P-39.1, la « LPRPSP ») à laquelle la Personne morale est assujettie;

ATTENDU QUE la LPRPSP, telle que modifiée par la Loi 25, prévoit que la personne ayant la plus haute autorité au sein de la Personne morale exerce la fonction de responsable de la protection des renseignements personnels à compter du 22 septembre 2022;

ATTENDU QUE [indiquer le titre de la personne ayant la plus haute autorité, par exemple le/la président.e, le/la directeur.trice général.e, le/la dirigeant.e] est la personne ayant la plus haute autorité au sein de la Personne morale;

ATTENDU QUE cette personne peut déléguer, par écrit, la fonction de responsable de la protection des renseignements personnels qu'elle assume à ce titre;

IL EST RÉSOLU :

1. **DE DÉLÉGUER** à [indiquer le nom et le titre de la personne à qui la délégation est faite] de la Personne morale, l'exercice des fonctions décrites à l'article 3.1 de la LPRPSP modifiée par la Loi 25 et ce, à compter du xx-xx-xxxx;

2. **DE CONSERVER** un exemplaire signé de la résolution ci-dessus dans le livre des procès-verbaux de la Personne morale.

[La page signature suit]

Incident de confidentialité

Depuis le **22 septembre 2022**, la Commission d'accès à l'information (« CAI »), mais aussi les personnes dont les renseignements personnels sont visés par un incident de confidentialité doivent être avisées, avec diligence, de tout incident impliquant de tels renseignements s'il y a des raisons de croire que cet incident présente un risque qu'un préjudice sérieux soit causé. Un registre des incidents de confidentialité doit aussi être tenu.

Qu'est-ce qu'un incident de confidentialité ?

On parle d'incident de confidentialité dans les cas suivants :

- Accès non autorisé par la loi à un renseignement personnel :
    - Consultation non autorisée des renseignements personnels par un employé ou par un fournisseur de service;
    - Intrusion d'un tiers dans le système informatique de l'entreprise: hameçonnage, rançongiciel, etc.;
    - Etc.
- Utilisation non autorisée par la loi d'un renseignement personnel :
    - Membre du personnel qui utilise des renseignements personnels d'une base de données à laquelle il a accès dans le cadre de ses fonctions dans le but d'usurper l'identité d'une personne;
    - Consultation / extraction non autorisée de renseignements personnels;
    - Etc.
- Communication non autorisée par la loi d'un renseignement personnel :
    - Communication de renseignements personnels à la mauvaise personne;
    - Etc.
- Perte d'un renseignement personnel ou toute autre atteinte à la protection d'un tel renseignement.

Un incident de confidentialité doit-il être déclaré à la Commission d'accès à l'information?

Oui, la CAI doit être avisée, avec diligence, d'un incident de confidentialité **si celui-ci présente un risque qu'un préjudice sérieux soit causé aux personnes** dont les renseignements personnels sont visés par cet incident.

Un formulaire est disponible sur le site de la CAI à cet effet.

Un incident de confidentialité doit-il être déclaré aux personnes concernées ?

Oui, les personnes dont les renseignements personnels sont visés par un incident doivent être avisées lorsque celui-ci présente un risque qu'un préjudice sérieux leur soit causé, à défaut de quoi la CAI peut ordonner de le faire.

Toutefois, si le fait de les aviser est susceptible d'entraver une enquête faite par une personne ou par un organisme qui, en vertu de la loi, est chargée de prévenir, détecter ou réprimer le crime ou les infractions aux lois, ils peuvent ne pas être avisés tout de suite.

Voir le Modèle de lettre publié par le Gouvernement du Québec (attention celui-ci fait référence à la Loi sur l'accès, il conviendra de faire les adaptations nécessaires) ou encore constituer son propre modèle de lettre qui doit contenir les éléments suivants :

- une description des renseignements personnels visés par l'incident ou, si cette information n'est pas connue, la raison justifiant l'impossibilité de fournir une telle description;
- une brève description des circonstances de l'incident;
- la date ou la période où l'incident a eu lieu ou, si cette dernière n'est pas connue, une approximation de cette période;
- une brève description des mesures que le membre a prises ou entend prendre à la suite de la survenance de l'incident, afin de diminuer les risques qu'un préjudice soit causé;
- les mesures que le membre suggère à la personne concernée de prendre afin de diminuer le risque qu'un préjudice lui soit causé ou afin d'atténuer un tel préjudice;
- les coordonnées permettant à la personne concernée de se renseigner davantage relativement à l'incident.

Comment déterminer si un incident de confidentialité présente un risque qu'un préjudice sérieux soit causé ?

Pour déterminer s'il y a un risque qu'un préjudice sérieux soit causé, il convient de considérer :

- La sensibilité du renseignement concerné.
    - Par ex., renseignement médical, financier ou encore d'identité, numéro d'assurance sociale.
- Les conséquences appréhendées de son utilisation.
    - Par ex., vol d'identité, fraude financière, atteinte à la réputation.
- La probabilité qu'il soit utilisé à des fins préjudiciables.
    - Par ex., les données ont-elles été exfiltrées des serveurs de l'organisme, publiées sur Internet ou encore sur le web caché (DarkWeb).

Est-ce qu'un membre peut communiquer avec un tiers (personne ou organisme) pour l'aider à diminuer le risque de préjudice ?

Oui, toute personne ou tout organisme susceptible d'aider à diminuer le risque de préjudice (police, assureur, avocat, entreprise d'investigation, etc.) peut être avisé.

Dans ce cas, seuls les renseignements nécessaires à cette fin peuvent être communiqués. La communication peut se faire sans le consentement des personnes concernées, mais le responsable de la protection des renseignements personnels doit enregistrer cette communication dans un registre.

Le responsable de la protection des renseignements personnels doit-il être consulté en cas d'incident de confidentialité ?

Oui, le responsable de la protection des renseignements personnels doit être avisé lors de l'évaluation du préjudice.

Un registre doit-il être tenu en cas d'incident de confidentialité ?

Oui, un registre des incidents de confidentialité doit être tenu et être transmis à la CAI sur demande. Voir le Modèle de registre publié par le Gouvernement du Québec (attention celui-ci fait référence à la Loi sur l'accès, il conviendra de faire les adaptations nécessaires) ou encore constituer son propre registre qui doit contenir les éléments suivants :

- Renseignements visés par l'incident;
- Circonstances de l'incident;
- Date ou période de l'incident;
- Date ou période de la prise de connaissance de l'incident;
- Nombre de personnes concernées par l'incident;
- Risque qu'un préjudice sérieux soit causé;
- Transmission des avis à la CAI et aux personnes concernées;
- Description des mesures prises par l'organisme.

Quelle est la durée de conservation du registre des incidents de confidentialité ?

En vertu du Règlement sur les incidents de confidentialité, les renseignements contenus au registre doivent être tenus à jour et conservés pendant une **période minimale de cinq ans** après la date ou la période au cours de laquelle le membre a pris connaissance de l'incident.

Mesures à prendre / Questions à se poser

- Établir un plan de gestion en cas d'incidents de confidentialité (voir modèle ci-joint), incluant :
    - Évaluation de la situation, identifier les mesures visant à diminuer les risques ou éviter qu'un incident de même nature se reproduise, identifier la nature du préjudice et, le cas échéant déclarer à la CAI et aux personnes concernées;
    - Intervenants : définition du rôle et responsabilité de chacun.
- Établir une grille d'analyse afin de déterminer le niveau de préjudice du risque susceptible d'être causé aux personnes concernées.
- Tenir un registre des incidents de confidentialité.

Mais aussi,

- Connaître la nature, les supports et la circulation des renseignements personnels détenus par ou pour le compte de l'organisme;
- Faire l'inventaire des mesures de sécurité en place (les réviser le cas échéant);
- Faire l'inventaire des contrats avec les tiers pour s'assurer qu'ils contiennent une clause à l'effet qu'en cas d'incident de confidentialité le responsable de la protection des renseignements doit être avisé;
- Réviser son contrat d'assurance afin d'ajouter, le cas échéant, une clause relative à la cybersécurité;

Pour aller plus loin : COMMISSION D'ACCÈS À L'INFORMATION, Incident de confidentialité

Modèle : Plan de gestion d'un incident de confidentialité

[Nom de l'entreprise] reconnaît l'importance d'assurer la protection des renseignements personnels qu'elle recueille auprès de sa clientèle, de ses employés et de toute autre personne avec qui elle est appelée à interagir dans le cadre de ses activités.

À ce titre, [Nom de l'entreprise] est responsable de la protection des renseignements personnels qu'elle détient ou qu'elle confie, le cas échéant, à un tiers, et ce, tout au long du cycle de vie de ces renseignements.

[Nom de l'entreprise] prends les mesures nécessaires pour assurer la protection des renseignements personnels. Néanmoins, des incidents de confidentialité impliquant des renseignements personnels peuvent survenir.

[Nom de l'entreprise] se dote du présent plan pour être en mesure de diminuer et de répondre adéquatement en cas d'incident de confidentialité.

1. Objectif et Cadre juridique

Le présent plan a pour objectif d'établir les démarches à suivre lorsque [Nom de l'entreprise] a des motifs de croire que s'est produit un incident de confidentialité impliquant des renseignements personnels qu'elle détient ou qu'elle a confiés à un tiers.

2. Cadre juridique

Le présent plan tient compte du cadre juridique applicable à [Nom de l'entreprise] en matière de protection des renseignements personnels, soit notamment la *Loi sur la protection des renseignements personnels dans le secteur privé* (RLRQ, c. P-39.1) et le *Règlement sur les incidents de confidentialité* (RLRQ, c. A-2.1, r. 3.1).

3. Champ d'application

Le présent plan s'applique aux employés, [indiquer si d'autres personnes ont accès aux renseignements personnels au sein de [Nom de l'entreprise], par exemple des membres de comités, administrateurs], mais aussi aux tiers auxquels [Nom de l'entreprise] communique des renseignements personnels, aux fournisseurs ou partenaires de [Nom de l'entreprise], incluant les sous-traitants.

4. Définition

Aux fins du présent plan, on entend par :

- **Incident de confidentialité** : tout accès, utilisation ou communication non autorisés par la loi d'un Renseignement personnel, ou toute perte ou autre atteinte à la protection de ce renseignement.

- *Exemples d'accès non autorisé par la loi :*
  - *Consultation non autorisée / non nécessaire à l'exercice des fonctions des renseignements personnels par un employé ou par un fournisseur de service ;*
  - *Intrusion d'un tiers dans le système informatique de l'entreprise : hameçonnage, rançongiciel, etc.*
  - *Etc.*

- *Exemples d'utilisation non autorisée par la loi :*
  - *Membre du personnel qui utilise des renseignements personnels d'une base de données à laquelle il a accès dans le cadre de ses fonctions dans le but d'usurper l'identité d'une personne ;*
  - *Consultation / extraction non autorisée de renseignements personnels ;*
  - *Etc.*

- *Exemples de communication non autorisée par la loi :*
  - *Communication de renseignements personnels à la mauvaise personne;*
  - *Etc.*

- **Personne concernée** : toute personne dont les Renseignements personnels sont visés par un Incident de confidentialité.
- **Personne liée** : employés, tiers auxquels [Nom de l'entreprise] communique des renseignements personnels, fournisseurs ou partenaires de [Nom de l'entreprise], incluant les sous-traitants.
- **Préjudice sérieux** : Acte ou évènement susceptible de porter atteinte à la Personne concernée ou à ses biens et de nuire à ses intérêts de manière non négligeable.
- **Renseignement personnel** : tout renseignement qui concerne une personne physique et qui permet, directement ou indirectement, de l'identifier.
- **Responsable de la protection des renseignements personnels** : personne veillant à assurer le respect et la mise en œuvre du cadre juridique applicable à la protection des renseignements personnels au sein de [Nom de l'entreprise].

5. Procédure à suivre

5.1. Signalement

Si une personne liée à [Nom de l'entreprise] a des raisons de croire qu'un incident de confidentialité impliquant des renseignements personnels s'est produit, elle doit en aviser, sans délai, le Responsable de la protection des renseignements personnels de [Nom de l'entreprise] et lui fournir toute information pertinente.

5.2. Évaluer la situation

Le Responsable de la protection des renseignements personnels doit :

- **Examiner** le signalement afin de **déterminer** s'il s'agit d'un incident de confidentialité impliquant des renseignements personnels.
    - *Exemples de questions à se poser :*
        - *Les informations visées par l'incident sont-elles des Renseignements personnels ?*
        - *Les Renseignements personnels ont-ils fait l'objet d'un accès, d'une utilisation ou d'une communication non autorisée par la loi ? ont-ils fait l'objet d'une perte ou de toute autre atteinte à leur protection ?*

- **Aviser** les intervenants concernés à l'interne afin d'identifier, de circonscrire, d'enquêter et de corriger la situation liée à l'incident de confidentialité.

    - [Intervenants concernés – à compléter par [Nom de l'entreprise] en fonction de la structure déterminée pour gérer les incidents avec le responsable de la PRP]
    - *Exemples de questions à se poser :*
        - *Quelle est la cause de l'incident ?*
        - *Quelle est la date ou la période visée par l'incident ?*
        - *Quels sont les renseignements personnels visés ?*
        - *Étaient-ils chiffrés / protégés par un mot de passe ?*
        - *Ont-ils été récupérés ou détruits ?*
        - *Qui sont les personnes concernées par l'incident ? Quel est leur nombre ?*
        - *Quelles sont les mesures de sécurité en place au moment de l'incident ?*

- **Aviser** la haute direction et/ou le conseil d'administration.

5.3. Diminuer les risques – limiter les atteintes à la vie privée

Le Responsable de la protection des renseignements personnels doit prendre rapidement les mesures raisonnables pour diminuer les risques qu'un préjudice soit causé et éviter que de nouveaux incidents de même nature ne se produisent.

- *Exemples de mesures à prendre :*
    - *Récupérer ou exiger la destruction des Renseignements personnels impliqués ;*
    - *Révoquer ou modifier les mots de passe ;*
    - *Cesser la pratique non autorisée ;*
    - *Corriger les lacunes des systèmes informatiques ;*
    - *Contacter les personnes ou organismes à l'externe susceptibles de diminuer le risque de préjudice.*

5.4. Identifier le risque de préjudice

Afin de déterminer si le préjudice est sérieux, le Responsable de la protection des renseignements personnels doit identifier le risque de préjudice en tenant compte :

- De la **sensibilité** des Renseignements personnels :
    - Renseignement de nature financière (Numéro de carte de crédit, de compte, de transit, information sur le soutien financier fourni par [Nom de l'entreprise] ou sur l'accommodation financière accordée, salaire, conditions d'emploi) ;
    - Renseignement de nature médicale ;
    - Renseignement d'identification (Numéro d'assurance sociale / maladie, permis de conduire) ;
    - Renseignement sur les origines ethniques, l'orientation sexuelle, l'identité de genre ;
    - Renseignement génétique ou biométrique ;
    - Etc.
- Des **conséquences appréhendées** de l'utilisation des Renseignements :
    - Vol d'identité ;
    - Fraude financière / Impact sur le dossier de crédit ;
    - Diffusion des renseignements personnels, notamment sensibles ;
    - Permanence / Perpétuation de l'atteinte ;
    - Répercussion sur la santé physique ou psychologique ;
    - Perte d'emploi ;
    - Humiliation, atteinte à la réputation, à la vie privée ;
    - Impact sur les relations professionnelles ou d'affaires ;
    - Etc.
- De la **probabilité** que les Renseignements soient utilisés à des fins préjudiciables.

Un formulaire est disponible au sujet de l'évaluation du risque de préjudice sérieux lors d'un incident de confidentialité.

5.5. Aviser les autorités compétentes et les personnes concernées

Le Responsable de la protection des renseignements personnels doit :

- **Aviser la CAI**, avec diligence, en cas de préjudice sérieux ;
- **Aviser les personnes** dont les Renseignements personnels sont visés par l'incident de confidentialité ;
- **Aviser les services de police ;**
- **Aviser les assureurs de** [Nom de l'entreprise] ;
- **Aviser les conseillers juridiques** pour obtenir des conseils relativement à la préservation de la preuve et aux risques juridiques associés aux mesures déployées ;
- Contacter les **personnes ou organismes à l'externe** susceptibles de diminuer le risque de préjudice. Si tel est le cas :

- Ne communiquer que les renseignements personnels à cette fin;
- Enregistrer la communication.

5.6. Tenir un registre des incidents de confidentialité

Le Responsable de la protection des renseignements personnels doit tenir un registre qui contient l'ensemble des incidents de confidentialité, et ce, peu importe que le risque ait été qualifié de sérieux ou non.

Les renseignements contenus au registre doivent être tenus à jour et conservés pendant une période minimale de 5 ans après la date ou la période au cours de laquelle [Nom de l'entreprise] a pris connaissance de l'incident.

5.7. Faire un suivi / un bilan de l'incident

Afin de tirer les leçons de l'incident de confidentialité, le Responsable de la protection des renseignements personnels doit :

- Approfondir l'analyse des circonstances de l'incident ;
- Documenter – de manière chronologique – les actions prises en lien avec l'incident ;
- Réviser les procédures en place et, le cas échéant, en adopter de nouvelles ;
- Sensibiliser les personnes liées à [Nom de l'entreprise] des mesures prises.

Transaction commerciale

Depuis le **22 septembre 2022**, si un membre est une partie à une transaction commerciale, par exemple une fusion-acquisition, il peut communiquer aux fins de cette transaction des renseignements personnels, mais seulement ceux nécessaires à cette fin. Cette communication doit se faire dans le cadre d'une entente précisant les obligations de chacune des parties à la transaction.

> **Pour aller plus loin** : COMMISSION D'ACCÈS À L'INFORMATION, Communication des renseignements personnels sans le consentement de la personne concernée, section incluant des éléments en lien avec les transactions commerciales.

Étude, recherche ou production de statistiques

Depuis le **22 septembre 2022**, un membre qui entend communiquer des renseignements personnels à une personne ou à un organisme qui souhaite utiliser ces renseignements à des fins d'étude, de recherche ou de production de statistiques doit, au préalable,

- réaliser une évaluation des facteurs relatifs à la vie privée ;
- conclure une entente avec cette personne ou organisme et la transmettre à la CAI. Cette entente entrera en vigueur 30 jours après sa réception par la CAI.

> **Pour aller plus loin** : COMMISSION D'ACCÈS À L'INFORMATION, Communication de renseignements personnels sans consentement à des fins de recherche, section incluant notamment des informations sur l'évaluation à réaliser, un modèle de formulaire à déposer à la CAI, un modèle d'engagement de confidentialité.

Biométrie

En vertu de la *Loi concernant le cadre juridique des technologies de l'information* (RLRQ, c. C-1.1) également modifiée par la Loi 25, si un membre entend recourir à un système biométrique pour vérifier ou confirmer l'identité des bénéficiaires, de fournisseurs, de ses employés, par exemple, au moyen d'un procédé biométrique, il doit depuis le **22 septembre 2022** déclarer à la CAI la banque de caractéristiques et de mesures biométriques au moins 60 jours avant sa mise en service.

Cette obligation de déclaration est déjà en vigueur, mais le délai pour le faire a été précisé par la Loi 25 et les autres obligations demeurent.

> **Pour aller plus loin** : COMMISSION D'ACCÈS À L'INFORMATION, Biométrie, section incluant notamment un Guide d'accompagnement quant aux principes à respecter et aux obligations légales (en révision), un modèle de formulaire de déclaration à déposer à la CAI, un modèle de formulaire de consentement à la collecte, à l'utilisation et à la conservation de renseignements biométriques.

Politiques et pratiques encadrant la gouvernance des renseignements personnels

Depuis le **22 septembre 2023**, un membre doit établir et mettre en œuvre des politiques et des pratiques encadrant sa gouvernance à l'égard des renseignements personnels et propres à assurer la protection de ceux-ci.

L'adoption de ces règles vise à encadrer les pratiques en matière de protection des renseignements personnels. Il est donc recommandé de répertorier l'ensemble des documents en lien avec la protection des renseignements personnels en vigueur afin de les réviser et, le cas échéant, d'en adopter de nouveaux pour répondre aux exigences de la Loi 25.

Ces règles sont le plus souvent énoncées dans des guides, politiques, procédures ou directives et sont diffusées pour permettre, tant à l'interne qu'à l'externe, de comprendre l'encadrement dont bénéficient les renseignements personnels. De plus, elles doivent être proportionnées à la nature et à l'importance des activités du membre.

Quelles sont les règles encadrant la gouvernance des renseignements personnels qui doivent être adoptées ? (Voir le modèle ci-joint)

Les membres doivent minimalement adopter des règles précisant :

- Le rôle et les responsabilités des membres du personnel tout au long du cycle de vie des renseignements personnels;
- Le processus de traitement des plaintes relatives à la protection des renseignements personnels;
- Les mesures applicables à la conservation et à la destruction des renseignements personnels.

Par ailleurs, il est recommandé également d'adopter ou à tout le moins de réviser les règles énonçant :

- Les mesures visant à assurer la sécurité des renseignements personnels, incluant le plan de gestion des incidents de confidentialité;
- L'utilisation et la communication des renseignements personnels afin notamment de préciser dans quels cas il convient de procéder à une évaluation des facteurs relatifs à la vie privée;
- Le processus de traitement des demandes d'accès et de rectification aux renseignements personnels;
- Les activités de formations et de sensibilisation offertes / reçues.

Qui doit approuver les règles encadrant la gouvernance à l'égard des renseignements personnels

Les politiques et pratiques encadrant la gouvernance des renseignements personnels doivent être approuvées par le responsable de la protection des renseignements personnels de l'entreprise.

Mesures à prendre / Questions à se poser

- Déterminer qui a accès aux renseignements personnels au sein de l'entreprise;
- Définir les rôles et responsabilités de chacune des personnes ayant accès aux renseignements personnels – en profiter pour revoir les accès et les mesures de sécurité applicables;
- Effectuer un inventaire des politiques, directives, pratiques et procédures en place relatives à la protection des renseignements personnels tout au long de leur cycle de vie, soit de leur collecte à leur destruction;
- Élaborer (ou réviser) le processus de traitement des plaintes :
    - Déterminer et diffuser auprès de qui et comment les plaintes sont adressées;
    - Déterminer le délai de traitement d'une plainte;
    - Description des différentes étapes du traitement;
        - Réception et accusé de réception / Évaluation de la plainte (prise de connaissance des documents et de la version des faits de chacune des parties) / Réponse à donner au plaignant (entente, mesures de redressement, fermeture du dossier).
    - Registre des plaintes.
- Élaborer (ou réviser) les mesures relatives à la conservation et à la destruction des renseignements personnels;
- Faire approuver les règles de gouvernance par le responsable de la protection des renseignements personnels de l'entreprise;
- Diffuser des informations détaillées en lien avec les politiques et pratiques encadrant la gouvernance des renseignements personnels.

Pour aller plus loin : COMMISSION D'ACCÈS À L'INFORMATION, Destruction et anonymisation, Procédure de destruction.

Modèle : Politique encadrant la gouvernance des renseignements personnels

1. Contexte et Champ d'application

La protection des renseignements personnels est importante pour [Nom de l'entreprise]. La présente *Politique encadrant la gouvernance des renseignements personnels* (« Politique ») adoptée en vertu du cadre juridique applicable à [Nom de l'entreprise] précise les pratiques quant à la gouvernance des renseignements personnels que nous détenons.

La présente politique s'adresse à l'ensemble du personnel de [Nom de l'entreprise]. Elle s'applique à tous les renseignements personnels détenus par [Nom de l'entreprise], y compris ceux dont la conservation est assurée par un tiers, quel que soit le support sur lequel ils sont conservés, et ce, de leur collecte à leur destruction. En ce sens, la présente politique s'applique également aux personnes avec qui [Nom de l'entreprise] fait affaire dans le cadre d'un mandat ou d'un contrat de service.

Par « renseignement personnel », nous entendons tout renseignement qui concerne une personne physique et permet, directement ou indirectement, de l'identifier.

2. Rôles et responsabilités du personnel de l'entreprise à l'égard des renseignements personnels

[Décrire les postes des personnes qui ont accès aux renseignements personnels détenus par l'entreprise : propriétaire, personnel administratif, technicien, stagiaire, etc., incluant le responsable de la protection des renseignements personnels]

2.1. Responsable de la protection des renseignements personnels

Chez [Nom de l'entreprise], la fonction de responsable de la protection des renseignements personnels est assurée par [indiquer le titre de la personne qui assume cette fonction].

Le responsable de la protection des renseignements personnels a pour responsabilité de veiller au respect et à la mise en œuvre des politiques et pratiques encadrant la gouvernance de [Nom de l'entreprise] à l'égard des renseignements personnels que nous détenons, et ce, afin de répondre aux exigences découlant du cadre juridique applicable en la matière.

À ce titre, il doit, entre autres :

- Veiller à assurer le respect et la mise en œuvre des dispositions de la Loi sur la protection des renseignements personnels dans le secteur privé ;
- Veiller à l'application de la présente Politique ;
- Être consulté lors de l'évaluation du risque qu'un préjudice soit causé à une personne dont un renseignement personnel est concerné par un incident de confidentialité ;
- Tenir les registres de communications de renseignements personnels, incluant en cas d'incident de confidentialité ;

- [Être consulté à toute étape d'une évaluation des facteurs relatifs à la vie privée en lien avec un projet visant un système d'exploitation ou de prestation électronique de services impliquant des renseignements personnels / la communication de renseignements personnels à l'extérieur du Québec / la communication à des fins d'étude, de recherche ou de production de statistiques – si applicable] ;
- Répondre aux demandes d'accès aux renseignements personnels et, le cas échéant, aux demandes de rectification. Il doit aussi prêter assistance au demandeur à comprendre la décision de lui refuser – en tout ou en partie – l'accès ou la rectification d'un renseignement personnel ;
- Répondre aux demandes de la Commission d'accès à l'information.

2.2. Personnel administratif

Notre personnel administratif [préciser] peut, dans l'exercice de ses fonctions, avoir accès aux renseignements personnels détenus par [Nom de l'entreprise]. À ce titre, le personnel doit :

- Respecter les règles que nous avons adoptées quant à la protection des renseignements personnels, et ce, tout au long de leur cycle de vie ;
- N'accéder qu'aux renseignements personnels nécessaires à l'exercice de ses fonctions ;
- Informer le responsable de la protection des renseignements personnels de tout incident ou tentative d'incident lié à la protection des renseignements personnels détenus par [Nom de l'entreprise] ;
- Participer aux activités de formation et de sensibilisation mises à leur disposition par [Nom de l'entreprise].

3. Protection des renseignements personnels

La protection des renseignements personnels tient une place importante au sein de [Nom de l'entreprise] et, nous prenons les mesures nécessaires pour faire en sorte que l'ensemble des personnes œuvrant au sein de [Nom de l'entreprise] adopte une attitude responsable tout au long du cycle de vie des renseignements personnels.

À ce titre, [Nom de l'entreprise] s'assure : [pour chacun des items suivants, possibilité de préciser davantage, notamment s'il y a des politiques qui peuvent publiées]

- De ne **collecter** que les renseignements personnels nécessaires à la réalisation de ses activités ;
- D'**informer** les personnes auprès de qui des renseignements personnels sont collectés des finalités de la collecte ;
- D'obtenir le **consentement** des personnes concernées quant à l'utilisation et la communication à des tiers de leurs renseignements personnels : voir le formulaire
-
- D'**utiliser** et de **communiquer** les renseignements personnels que dans les limites prescrites par le cadre juridique applicable en la matière ;
- De prendre les **mesures de sécurité** propres à assurer la protection des renseignements personnels compte tenu de leur sensibilité, de la finalité de leur utilisation, de leur quantité, de leur répartition et de leur support ;

- De prendre les mesures raisonnables pour diminuer les risques qu'un préjudice soit causé aux personnes dont les renseignements personnels sont visés par un **incident de confidentialité** et éviter qu'un incident de même nature ne se produise ;
- De prendre des mesures raisonnables afin de respecter les exigences en matière de **conservation et de destruction** des renseignements personnels.

4. Demande d'accès ou de rectification des renseignements personnels

Si une personne souhaite connaître les renseignements personnels que [Nom de l'entreprise] détient sur elle ou encore si elle veut procéder à une rectification de ceux-ci, elle doit s'adresser, par écrit, au responsable de la protection des renseignements personnels à l'adresse suivante [indiquer l'adresse postale et courriel du responsable].

5. Plainte relative à la protection des renseignements personnels

Advenant le cas où une personne souhaite déposer une plainte quant à la protection que [Nom de l'entreprise] accorde aux renseignements personnels que nous détenons, celle-ci peut le faire en contactant le responsable de la protection des renseignements personnels [préciser le moyen : par courriel à l'adresse suivante : […] ; en remplissant le formulaire électronique prévu à cet effet et disponible à l'adresse suivante : […] ; par la poste à l'adresse suivante : […] ; etc.]

La plainte doit minimalement contenir les éléments suivants :

- Identification du plaignant : nom, coordonnées [préciser si : postale, téléphonique, et/ou électronique] ;
- Objet et motif de la plainte – la plainte doit suffisamment être précise, dans le cas contraire le responsable de la protection des renseignements personnels pourra communiquer avec le plaignant pour obtenir toute information supplémentaire afin d'être en mesure d'évaluer la plainte.

Le responsable de la protection des renseignements personnels doit, avec diligence et au plus tard dans les [indiquer le nombre de jours] qui suivent la réception de la plainte traiter celle-ci et informer le plaignant des conclusions de celles-ci.

6. Mise à jour de la Politique

[Nom de l'entreprise] veille à réviser la présente Politique tous les [indiquer la fréquence] ou plus rapidement lors de modifications législatives.

Évaluation des facteurs relatifs à la vie privée

Une évaluation des facteurs relatifs à la vie privée (« **EFVP** ») permet d'anticiper les risques d'atteinte à la vie privée des personnes concernées et de prendre les mesures pour les atténuer et ainsi se conformer aux exigences légales en matière de protection des renseignements personnels.

> **Pour aller plus loin** : COMMISSION D'ACCÈS À L'INFORMATION, Guide d'accompagnement – Réaliser une évaluation des facteurs relatifs à la vie privée, 2023; GOUVERNEMENT DU QUÉBEC, Évaluation des facteurs relatifs à la vie privée (**Note** : cette page vise les organismes assujettis à la Loi sur l'accès. Toutefois, elle peut être consultée en faisant les adaptations nécessaires).

Dans quel cas doit-on réaliser une EFVP?

Une EFVP doit être réalisée dans les cas suivants par les membres:

- Depuis le **22 septembre 2022**, une EFVP doit être réalisée avant de communiquer des renseignements personnels sans le consentement des personnes concernées à une personne ou à un organisme qui souhaite utiliser ces renseignements à des fins d'étude, de recherche ou de production de statistiques;
- Depuis le **22 septembre 2023**, une EFVP devra être réalisée:
    - 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;
        - **Note** : La mise à jour d'un système d'information ou de prestation électronique n'est pas visée par cette exigence, sauf si la mise à jour à une incidence importante sur la protection des renseignements personnels.
    - Avant de communiquer à l'extérieur du Québec un renseignement personnel ou de confier à une personne ou un organisme à l'extérieur du Québec la tâche de recueillir, d'utiliser, de communiquer ou de conserver pour son compte un tel renseignement.

Quels sont les éléments à prendre en considération dans le cadre d'une EFVP?

Chacun des cas dans lequel une EFVP doit être réalisée prévoit des éléments spécifiques. Néanmoins, doivent être pris en considération :

- La sensibilité des renseignements personnels;
- La finalité de leur utilisation;
- Leur quantité, leur répartition et leur support.

Pour ce qui est des EFVP à réaliser avant de communiquer des renseignements à l'extérieur du Québec, il convient également de considérer les mesures de protection dont le renseignement bénéficiera, ainsi que le régime juridique applicable dans l'État où les renseignements sont communiqués. De plus, une entente doit être conclue entre les parties.

À quel moment doit être réalisée une EFVP?

Une EFVP doit être réalisée **avant** tout projet d'acquisition, de développement ou de refonte et **avant** de communiquer les renseignements personnels à l'extérieur du Québec ou à des fins d'étude, de recherche ou de production de statistiques.

Une EFVP doit donc être réalisée en amont de ces trois cas de figure.

Un rapport / document en lien avec l'EFVP doit-il être rédigé?

Oui, un rapport doit être produit afin de permettre à toute personne qui n'aurait pas été impliquée dans l'évaluation de comprendre quel est le projet, comment il est susceptible d'affecter la vie privée et quelles sont les mesures qui ont été prises pour atténuer les risques.

Ce rapport pourrait contenir les éléments suivants:

- Quel est le projet? Quelle est sa finalité?
    - Étude, recherche, production de statistiques;
    - Acquisition, développement, refonte;
    - Communication hors Québec.
- Quels sont les renseignements personnels nécessaires pour réaliser le projet?
    - Nom, Prénom;
    - Adresse (postale, courriel, IP, …);
    - Numéro de téléphone;
    - NAS, NAM;
    - Renseignements démographiques;
    - Etc.
- Quel est le niveau de sensibilité des renseignements personnels?
    - Si renseignement sensible – un consentement manifesté de manière expresse a-t-il été obtenu?
- Comment les renseignements personnels sont-ils recueillis?
- Quelles sont les personnes qui auront accès aux renseignements personnels?
    - Au sein de l'établissement;
    - À l'extérieur de l'établissement.
- Sur quel(s) support(s) les renseignements personnels sont conservés? Hébergés?
- Les renseignements sont-ils communiqués / confiés à l'extérieur du Québec?

    - Si oui – quels sont les éléments pris en considération pour évaluer l'adéquation du pays destinataire des renseignements personnels?
- Un contrat a-t-il été conclu avec le fournisseur de service externe?
    - Si oui, une clause doit être prévue à l'égard des sous-traitants, des obligations de chacune des parties, des obligations en matière d'assurance et d'audit notamment.
- Quelles sont les mesures de sécurité mises en place pour assurer la protection des renseignements personnels?
- Quels sont les risques identifiés? Et quelles sont les probabilités qu'ils se réalisent?
- Quelles sont les mesures prises pour minimiser les risques pour les personnes concernées?
- Quels sont les moyens et les stratégies mis en place pour assurer le respect des obligations et des principes de protection des renseignements personnels ?
- Quelles sont les mesures prises en lien avec la conservation et la destruction des renseignements personnels?
- Est-ce qu'un processus de vérification et de correction des renseignements personnels est prévu?
- Quel est le suivi prévu? Par qui?

Le responsable de la protection des renseignements personnels de l'entreprise doit-il être consulté?

Oui, le responsable doit être consulté dans le cadre d'une EFVP.

Mesures à prendre / Questions à se poser

- Faire l'inventaire des systèmes d'information et de prestation électronique de services et des projets pour lesquels des renseignements personnels sont communiqués à des tiers.
- Faire l'inventaire des contrats avec les fournisseurs de services et, le cas échéant, les réviser.
- Déterminer si des renseignements personnels sont communiqués à l'extérieur du Québec et, le cas échéant s'assurer de la protection accordée et réviser le contrat avec le fournisseur.
- Définir un cadre de gestion des projets et une méthodologie qui permettent notamment d'évaluer les facteurs relatifs à la vie privée et de gérer les risques en matière de protection des renseignements personnels.

Consentement – Information – Politique de confidentialité

Un consentement doit être **manifeste, libre et éclairé**. Il doit être **donné à des fins spécifiques** et il **ne vaut que pour la durée nécessaire à la réalisation des fins pour lesquelles il a été demandé**.

> **Note** : Le consentement donné pour l'utilisation à d'autres fins ou la communication à des tiers de **renseignements personnels sensibles**, comme ceux de santé par exemple, doit être **manifesté de façon expresse**.
>
> **Note** : En ce qui concerne les **mineurs de moins de 14 ans**, le consentement est donné par le titulaire de l'autorité parentale ou par le tuteur. En ce qui concerne les **mineurs de 14 ans et plus**, le consentement peut être donné par le mineur, le titulaire de l'autorité parentale ou par le tuteur.

Depuis le **22 septembre 2023**, il est prévu que le consentement doit être demandé pour chacune des fins envisagées. Ainsi, une personne peut consentir à fournir ses renseignements personnels pour avoir accès aux services fournis par un membre, ce qui ne signifie pas forcément que cette personne consent à ce que ses renseignements personnels soient utilisés ou communiqués à des tiers à d'autres fins.

Cela ne signifie pas que la demande doit être présentée sur un document à part, cela signifie qu'elle ne doit pas se fondre avec toutes les autres informations. (Voir modèle ci-joint)

Quelles sont les informations à communiquer ?

Parmi les informations à transmettre lors de la collecte des renseignements personnels, il est prévu que les personnes concernées doivent être informées, entre autres :

- des fins auxquelles les renseignements sont recueillis ;
- des moyens par lesquels ils le sont;
- des droits d'accès et de rectification reconnus aux personnes concernées ;
- du droit de retirer le consentement à l'utilisation et à la communication des renseignements recueillis.

Les personnes concernées doivent aussi informées, le cas échéant, du nom des tiers ou des catégories de tiers à qui il est nécessaire de communiquer les renseignements recueillis pour les fins décrites ou encore de la possibilité que les renseignements soient communiqués à l'extérieur du Québec.

> **Note** : Si un membre entend avoir recours à une technologie comprenant des fonctions permettant d'identifier, de localiser ou de profiler les bénéficiaires ou encore ses employés, il doit les informer au préalable et leur indiquer les moyens offerts pour activer ces fonctions.
>
> **Note** : Si un membre entend rendre une décision à l'égard d'un bénéficiaire fondée exclusivement sur un traitement automatisé, il doit l'informer des renseignements utilisés, des raisons et facteurs ayant mené à la décision et de son droit de faire réviser la décision.

Les personnes concernées doivent également être informées, sur demande, des renseignements personnels recueillis, des personnes qui y auront accès au sein de l'organisme, de leur durée de conservation et des coordonnées de la personne responsable des renseignements personnels.

Comment diffuser les informations à communiquer ?

Il est prévu qu'un membre qui recueille des renseignements personnels par un moyen technologique doit publier sur son site Internet une politique de confidentialité, laquelle reprend généralement les éléments décrits précédemment.

Cette politique peut également être diffusée par tout autre moyen, par exemple une affiche, un feuillet d'information ou encore une annexe au formulaire de consentement, advenant le cas où le membre n'a pas de site Internet.

Mesures à prendre / Questions à se poser

- Faire l'inventaire des renseignements collectés, utilisés et communiqués;
- Faire l'inventaire des formulaires de consentement et, le cas échéant, les réviser;
- Réviser (ou adopter) la politique de confidentialité. (Voir modèle ci-joint).

Pour aller plus loin : COMMISSION D'ACCÈS À L'INFORMATION,
Lignes directrices – Consentement – critères de validité

Modèle : Consentement à un traitement ostéopathique

Modèle tiré du formulaire de consentement proposé par Ostéopathie Québec.

1. Consentement

- Je reconnais, par la présente, que [Prénom Nom], ostéopathe et membre en règle d'Ostéopathie Québec, m'a expliqué la nature du problème, la nécessité du traitement retenu, les effets bénéfiques escomptés ainsi que les effets secondaires et risques possibles en lien avec ce traitement.
- Je consens volontairement et librement à ce que l'ostéopathe procède au traitement discuté, en tenant compte de ma condition physique et de mon état de santé général.
- Je m'engage à informer l'ostéopathe de tout changement de mon état de santé ou de ma condition physique qui surviendrait en cours de traitement.
- Je comprends que ce consentement est donné pour toute la durée du traitement ostéopathique, c'est-à-dire pour toutes les séances en lien avec ledit traitement, à moins d'une indication contraire de ma part.
- Je déclare avoir été informé(e) qu'il m'est possible de révoquer mon consentement en tout temps et également de refuser toute manipulation ostéopathique qui ne me convient pas.
- Je consens à ce qu'il/elle utilise mes renseignements personnels (nom, prénom, coordonnées postale / électronique / téléphonique) pour me transmettre des informations générales en lien avec l'ostéopathie en général. (Attention, cette mention doit être ajoutée au formulaire que si c'est une pratique, si ce n'est pas le cas, ne pas l'ajouter au formulaire de consentement au traitement).

_____

Nom du client (Lettre moulées)

_____ _____

Signature (client ou représentant légal) Date

2. Engagement de l'ostéopathe

Je reconnais avoir transmis toutes les informations relatives aux techniques ostéopathiques qui seront utilisées dans le cadre du traitement, dont leur nature, les raisons justifiant leur utilisation, leurs bienfaits, leurs effets secondaires ainsi que leurs possibles risques.

_____ _____

Nom de l'ostéopathe (Lettres moulées) No de membre

_____ _____

Signature Date

Modèle : Politique de confidentialité

[Nom de l'entreprise] reconnaît l'importance d'assurer la protection des renseignements personnels qu'elle recueille via son site Internet ou par tout autre moyen technologique.

À ce titre, [Nom de l'entreprise], est responsable de la protection des renseignements personnels qu'elle détient ou qu'elle confie, le cas échéant, à un tiers.

Par « renseignements personnels », il convient d'entendre tout renseignement qui concerne une personne physique et qui permet, directement ou non, de l'identifier.

La présente *Politique de confidentialité* s'applique à toute personne qui visite notre site Internet et utilise les différents services qui y sont présentés ou interagit avec nous par le biais de celui-ci ou de tout autre moyen technologique.

Elle fait état de la manière dont [Nom de l'entreprise] protège vos renseignements personnels, et ce, afin de tenir compte des exigences des lois applicables en la matière au Québec, à savoir *Loi sur la protection des renseignements personnels dans le secteur privé* (RLRQ, c. P-39.1).

1) **Renseignements personnels que nous recueillons :**

Dans le cadre de vos interactions avec nous, [Nom de l'entreprise] recueille certains renseignements personnels vous concernant. Les renseignements personnels que nous recueillons sont nécessaires afin de vous offrir les services demandés. Ces renseignements varient en fonction des personnes auprès de qui ils sont recueillis :

- ***Décrire les renseignements personnels recueillis :*** [*nom, coordonnées, renseignement nécessaire pour traiter une demande, navigateur web, adresse IP, pages visitées et requêtes, heure et jour de connexion, etc.]*

2) **Finalité de la collecte *:*** [Nom de l'entreprise] recueille vos renseignements personnels pour atteindre les objectifs décrits ci-dessous.

- ***Décrire les finalités***

3) **Moyens par lesquels vos renseignements personnels sont recueillis :**

[Nom de l'entreprise] recueille vos renseignements personnels par le biais [à compléter en fonction des moyens utilisés : site Internet, courriel, témoins de connexion dits « essentiels », plateformes de nos fournisseurs externes, etc.]

4) Consentement

En visitant notre site Internet ou encore en nous fournissant des renseignements personnels (par courriel, en remplissant un de nos formulaires en ligne, par téléphone, par nos réseaux sociaux), [Nom de l'entreprise] considère que vous consentez à leur utilisation et à leur communication aux fins mentionnées ci-dessus.

Vous pouvez en tout temps retirer votre consentement à l'utilisation et à la communication des renseignements personnels collectés par [Nom de l'entreprise]. Vous pouvez exercer votre droit en communiquant avec nous à l'adresse suivante [indiquer l'adresse à laquelle la demande de retrait peut être faite]. Le retrait de votre consentement pourrait nous empêcher de vous fournir ou de continuer à vous fournir certains de nos services.

5) Utilisation et Communication

En aucun cas, [Nom de l'entreprise] n'utilise ni ne communique vos renseignements personnels sans votre consentement. Toutefois, [Nom de l'entreprise], peut être tenu de communiquer vos renseignements personnels à des tiers, sans votre consentement, lorsque la loi nous le permet, par ex : aux autorités qui ont le droit de les exiger, pour se conformer à toute ordonnance d'un tribunal ou encore si nous croyons que la communication est nécessaire en raison d'une situation d'urgence mettant en danger la vie, la santé ou la sécurité de la personne concernée ou encore pour prévenir un acte de violence, dont un suicide.

Possibilité d'ajouter, le cas échéant

De plus, nous partageons vos renseignements personnels avec nos partenaires à des fins de [indiquer les fins étant entendu que celles-ci ne peuvent aller à l'encontre des situations prévues par la législation applicable + indiquer les catégories de tiers].

En pareille situation, [Nom de l'entreprise] s'assure contractuellement que les tiers respectent la confidentialité de vos renseignements personnels, ne les utilisent pas à d'autres fins que celles pour lesquelles ils leur ont été communiqués et les gèrent conformément au cadre juridique applicable en la matière.

6) Conservation des renseignements personnels

[Nom de l'entreprise] conserve vos renseignements personnels uniquement pendant la durée nécessaire pour réaliser les fins pour lesquelles ils ont été collectés, sauf lorsque la loi prévoit une durée de conservation différente pour répondre aux exigences légales.

En général vos renseignements personnels sont traités et hébergés au Québec. ***Possibilité d'ajouter :*** Toutefois, dans le cas, où ceux-ci seraient communiqués ou hébergés à l'extérieur, [Nom de l'entreprise] s'assure que vos renseignements personnels sont protégés de manière adéquate et que le transfert est prévu par entente.

7) Mesures de sécurité

[Nom de l'entreprise] protège vos renseignements personnels par des mesures de sécurité appropriées à la nature de ceux-ci et ce, afin d'éviter qu'une personne puisse y avoir accès, les utiliser, les communiquer à des tiers alors qu'elle n'y était pas autorisée ou encore afin de prévenir les pertes ou toute autre atteinte à la protection de ceux-ci.

Nous avons pris des mesures pour faire en sorte que seuls les membres de notre personnel qui doivent avoir accès à vos renseignements personnels dans le cadre de leurs fonctions soient autorisés à y accéder. Nous nous assurons également que les tiers à qui nous communiquons vos renseignements personnels prennent les mesures pour assurer le caractère confidentiel des renseignements que nous lui confions et qu'ils ne les utilisent que pour les fins prévues à l'entente conclue avec lui.

8) Accès et rectification à vos renseignements personnels

Il est important que les renseignements personnels que nous détenons à votre sujet soient à jour. Veuillez nous informer de tout changement quant à ceux-ci.

De plus, vous pouvez soumettre une demande :

- d'accès à vos renseignements personnels;
- de rectification de vos renseignements personnels;
- de retrait de votre consentement à l'utilisation ou à la communication de vos renseignements personnels;
- de cessation de la diffusion de vos renseignements personnels, de désindexation;
- de portabilité (à partir du 22 septembre 2024).

En vous adressant à [indiquer le titre et les coordonnées du responsable de la protection des renseignements personnels] par le biais [indiquer le moyen : formulaire en ligne, papier ou par courriel].

9) Porter plainte

Nous reconnaissons l'importance de protéger vos renseignements personnels. Advenant le cas où vous souhaitez déposer une plainte quant à la protection que [Nom de l'entreprise] accorde aux renseignements personnels qu'elle détient, vous pouvez le faire en contactant notre responsable de la protection des renseignements personnels [préciser le moyen : par courriel à l'adresse suivante : […] ; en remplissant le formulaire prévu à cet effet ; etc.]

10) Nous contacter

Vous pouvez communiquer avec nous au sujet de la présente *Politique de confidentialité* ou encore formuler des commentaires, exercer vos droits, déposer une plainte en vous adressant à [indiquer le titre et les coordonnées du responsable de la protection des renseignements personnels].

Date de la politique [entrée en vigueur, mise à jour]

Droit des personnes concernées

En vertu du cadre juridique applicable aux membres d'Ostéopathie Québec, une personne concernée, à savoir un patient ou encore un employé (actuel ou ancien) se voit reconnaître différents droits à l'égard de ses renseignements personnels, incluant entre autres le :

- **Droit d'accès et de rectification** : Une personne concernée peut vous demander de lui confirmer l'existence et l'accès aux renseignements personnels que vous détenez à son sujet et, le cas échéant, en demander la rectification. Ces droits d'accès et de rectification s'exercent quelle que soit la forme sous laquelle les renseignements personnels sont accessibles : écrite, sonore, visuelle ou encore informatisée.

- **Droit en lien avec un processus de deuil** : Le (la) conjoint.e ou un proche parent d'une personne décédée peut demander à ce que vous lui communiquez un renseignement personnel qu'il détient concernant la personne décédée, si la connaissance de ce renseignement est susceptible d'aider le requérant dans son processus de deuil et que la personne décédée n'a pas consigné par écrit son refus d'accorder ce droit d'accès.

Note : On entend par « conjoint », les personnes liées par un mariage ou une union civile, mais aussi les conjoints de fait.
On entend par « proche parent », les ascendants et les descendants directs, mais aussi les frères et les sœurs, les cousin.e.s, les tantes et les oncles entre autres.

La demande peut concerner, par exemple, un renseignement qui permet de comprendre les circonstances du décès ou encore un renseignement qui permet de se souvenir de la personne décédée (une photo). Dans le cas d'une telle demande, il vous revient de faire une évaluation au cas par cas en tenant compte du contexte de la demande pour apprécier si le renseignement est susceptible d'aider au processus de deuil.

Pour aller plus loin : GOUVERNEMENT DU QUÉBEC, Infographie – Communication d'un renseignement personnel susceptible d'aider une conjointe, un conjoint ou un proche parent dans son processus de deuil (**Note** : cette infographie vise les organismes assujettis à la Loi sur l'accès. Toutefois, elle peut être consultée en faisant les adaptations nécessaires).

- **Droit à la cessation de la diffusion d'un renseignement personnel ou encore à la désindexation de tout hyperlien rattaché à un nom permettant d'accéder à ce renseignement** : Une personne concernée peut exiger d'un membre d'Ostéopathie Québec qu'il cesse la diffusion d'un renseignement personnel la concernant ou que l'hyperlien permettant d'accéder à ce renseignement soit désindexé lorsque la diffusion de ce renseignement contrevient à la loi ou à une ordonnance judiciaire.

- **Droit à la portabilité** : À compter du **22 septembre 2024**, une personne concernée pourra obtenir d'un membre d'Ostéopathie Québec, dans un format technologique structuré et couramment utilisé, un renseignement personnel informatisé recueilli auprès d'elle par le membre d'Ostéopathie Québec (ou pour le compte de ce membre). Cette communication pourra aussi se faire à une personne ou à un organisme autorisé à recueillir un tel renseignement, à la demande de la personne concernée.

Est-ce que le droit à la portabilité s'applique aux renseignements personnels recueillis en format papier ?

Non, le doit à la portabilité est **limité aux renseignements personnels informatisés** recueillis auprès de la personne concernée. Ce droit s'applique donc aux renseignements déposés par la personne dans son dossier électronique ou encore à ceux relatifs à l'historique de ses rendez-vous, aux données enregistrées par une montre connectée.

Est-ce que je dois répondre à une telle demande si son traitement soulève des difficultés pratiques sérieuses ?

Le droit à la portabilité s'exerce **uniquement s'il ne soulève pas de difficultés pratiques sérieuses**, lesquelles peuvent venir notamment de la complexité que nécessite le transfert des données ou encore des coûts élevés qui pourraient être engendrés.

Si un membre d'Ostéopathie Québec invoque un tel motif pour refuser de donner suite à ce droit il doit être en mesure de fournir les justifications nécessaires en cas de recours devant la Commission d'accès à l'information.

Que faut-il entendre pas « format technologique structuré et couramment utilisé » ?

Un format est dit « structuré et couramment utilisé » lorsque des applications logicielles d'usage courant peuvent facilement reconnaître et extraire les informations qui y sont contenues. De manière générale, des formats ouverts de type CSV, XML ou JSON sont adaptés à la portabilité. En revanche, un format difficile à traiter, comme une image, un PDF ou un format dont l'utilisation implique l'acquisition d'un logiciel ou d'une licence payante, n'est pas considéré comme étant un format technologique structuré et couramment utilisé.

Si la personne demande un format particulier, le membre d'Ostéopathie Québec doit en tenir compte, sauf si ce choix soulève des difficultés pratiques sérieuses.

Dans tous les cas mentionnés ci-dessus, le responsable de la protection des renseignements personnels doit s'assurer de la qualité de la personne qui fait la demande, doit répondre à la demande dans un délai de 30 jours, doit motiver son refus de donner suite à une demande, doit indiquer les droits de recours devant la Commission d'accès à l'information.

Pour aller plus loin : *Loi sur la protection des renseignements personnels dans le secteur privé*, art. 27 et suivants.

Sanctions administratives pécuniaires – Amendes – Dommages-Intérêts

En cas de non-respect de l'une des obligations prévues par la LPRPSP, des sanctions administratives pécuniaires ou des amendes peuvent être émises par la CAI. Un tribunal peut aussi prononcer des dommages-intérêts.

Les montants en pareil cas sont :

	LPRPSP
Sanction administrative pécuniaire	50 000 $ dans le cas d'une personne physique et, dans les autres cas, de 10 000 000 $ ou du montant correspondant à 2 % du chiffre d'affaires mondial de l'exercice financier précédent si ce dernier montant est plus élevé. **Pour aller plus loin** : COMMISSION D'ACCÈS À L'INFORMATION, Cadre général d'application des sanctions administratives pécuniaires
Amende	5000 $ à 100 000 $ dans le cas d'une personne physique et, dans les autres cas, de 15 000 $ à 25 000 000 $ ou du montant correspondant à 4 % du chiffre d'affaires mondial de l'exercice financier précédent si ce dernier montant est plus élevé.
Dommages-intérêts	Au moins 1000 $.

Conservation des documents : bonnes pratiques

1. Sensibilisation du personnel

- Formez régulièrement votre personnel sur les meilleures pratiques en matière de protection des renseignements personnels.
- Assurez-vous que tous les employés comprennent l'importance de protéger les renseignements personnels des clients.
- Faites signer une politique de confidentialité à tous vos employés.

2. Collecte

- Ne collectez que les renseignements personnels nécessaires des clients.

3. Consentement

- Obtenez le consentement explicite des clients pour collecter et utiliser leurs renseignements personnels. Expliquez clairement comment ces données seront utilisées.
- Révisez vos documents pour vous assurer qu'ils sont conformes.

4. Sécuriser vos documents

- Stockez les documents physiques contenant des renseignements personnels dans un endroit sécuritaire, comme une pièce sécurisée et verrouillée ou un classeur verrouillé.

5. Contrôle des accès

- Limitez l'accès aux documents contenant des renseignements personnels uniquement aux employés autorisés qui en ont besoin pour accomplir leurs tâches.
- Mettez en place des politiques de gestion des accès pour contrôler qui peut accéder aux informations sensibles.

6. Politique de conservation des données

- Établissez une politique de conservation des données claire, indiquant combien de temps les documents contenant des renseignements personnels doivent être conservés.

7. Destruction

- Lorsque les documents ne sont plus nécessaires, détruisez-les de manière sécuritaire à l'aide d'un broyeur de documents ou d'un service de destruction de documents professionnel.

8. Surveillance

- Effectuez régulièrement des audits internes pour vous assurer que les pratiques de protection des renseignements personnels sont suivies.
- Surveillez les accès aux données pour détecter toute activité suspecte.

9. Transparence

- Informez vos clients, fournisseurs et employés de la manière dont leurs données seront utilisées et assurez-vous de répondre à toutes leurs questions concernant la protection de leurs renseignements personnels.