**Me Cynthia Chassigneux**
*Avocate, Langlois Avocats*

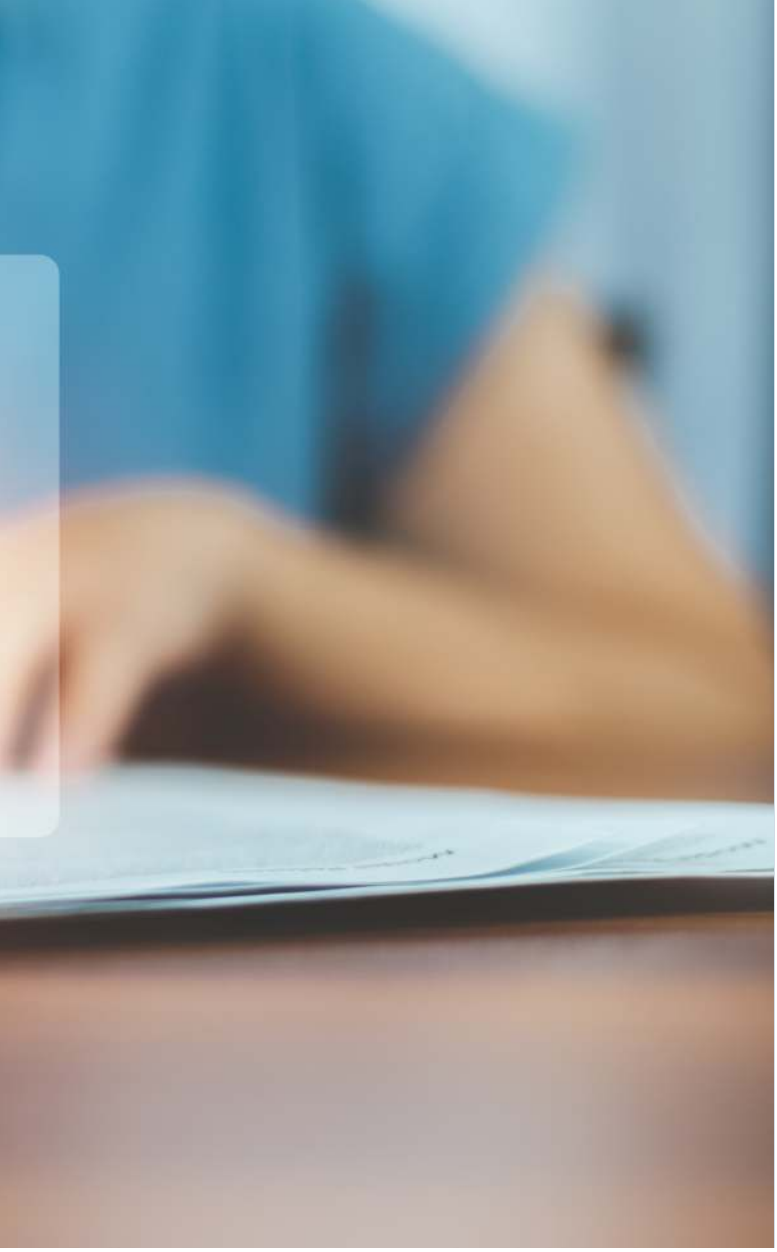
# Protection des renseignements personnels à la lumière de la Loi 25

Qui dit modernisation des dispositions législatives en matière de protection des renseignements personnels (« **PRP** »), dit nouvelles exigences pour les membres de l'Ordre des diététistes-nutritionnistes du Québec, mais aussi nouveaux droits pour le personnel ou les clients des diététistes-nutritionnistes.

La *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*[7] vient modifier et ajouter plusieurs articles à la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*[8] et à la *Loi sur la protection des renseignements personnels dans le secteur privé*[9]. Ces articles entrent en vigueur les 22 septembre 2022, 2023 et 2024.

7. LQ 2021, c. 25, la « **Loi 25** ».
8. RLRQ, c. A-2.1.
9. RLRQ, c. P-39.1, la « **LPRPSP** ».

À propos de l'auteure



Cette modernisation ne modifie pas les règles prévues au *Code des professions*[10] ou encore au *Code de déontologie des diététistes*[11], notamment en matière de respect du secret professionnel. Néanmoins, il est important que les diététistes-nutritionnistes considèrent les exigences de la Loi 25 dans leur pratique et ce, qu'ils exercent seuls ou à plusieurs au sein de cabinets privés, de firmes de consultants ou encore d'organismes à but non lucratif (« **organisations** »). La Loi 25 modernise le régime applicable à la protection des renseignements personnels dans tous les secteurs d'activités.

Le présent article présente sommairement certaines mesures à considérer pour pouvoir répondre aux exigences de la Loi 25 qui viennent modifier la LPRPSP.

## Responsabilité et Incident de confidentialité : deux des exigences qui sont entrées en vigueur en 2022

La Loi 25 reconnaît formellement qu'une entreprise est « **responsable** de la protection des renseignements personnels qu'elle détient » (art. 3.1), **que leur conservation soit assurée par l'entreprise ou par un tiers** (art. 1). Pour assurer le respect et la mise en œuvre de la LPRPSP au sein d'une organisation, la Loi 25 prévoit que la personne ayant la plus haute autorité au sein d'une organisation assume la fonction de **responsable de la PRP** (art. 3.1).

Cette fonction peut être déléguée, par écrit, en tout ou en partie, à toute personne au sein d'une organisation, mais aussi à l'externe. La *Loi 25* ne précise ni la forme, ni le

10. RLRQ, c. C-26.
11. RLRQ, c. C-26, r. 97.

**22/9/2022**

- Responsabilité et Responsable de la protection des renseignements personnels
- Déclaration des incidents de confidentialité
- Communication nécessaire aux fins de la conclusion d'une transaction commerciale, sans le consentement de la personne concernée
- Communication de renseignements personnels sans le consentement des personnes concernées à des fins d'étude, de recherche ou de production de statistiques
- Biométrie

**22/9/2023**

- 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
- Cessation de diffusion — Désindexation
- Destruction / Anonymisation
- Sanctions administratives précuniaires — Amendes — Dommages-Intérêts

**22/9/2024**

- Droit à la portabilité

contenu de cette délégation, ni le profil requis pour exercer cette fonction, ni si la personne désignée à l'externe doit ou non être située au Québec.

Le titre et les coordonnées du responsable de la PRP doivent être accessibles aux clients d'une organisation (c.-à-d. site Internet, contrat de services professionnels, feuillets, etc.). S'il est important de savoir qui sera responsable de la PRP au sein d'une organisation, il est tout aussi important de préciser que ce dernier doit, entre autres, être informé des **incidents de confidentialité** impliquant des renseignements personnels (RP). Il doit être consulté lors de l'évaluation du risque de préjudice (art. 3.7).

Depuis le 22 septembre 2022, une organisation – par le biais de son responsable de la PRP – doit aviser[12], avec diligence, la Commission d'accès à l'information mais aussi les personnes[13] dont les RP sont visés, de tout incident de confidentialité impliquant de tels renseignements s'il a des raisons de croire que cet incident présente un risque qu'un préjudice sérieux soit causé (art. 3.5), sous peine d'une sanction administrative pécuniaire (art. 90.1) ou d'une amende en cas d'omission (art. 91).

**Actions :**

Faire un inventaire des RP, des politiques et procédures en place ou encore des contrats avec les différents prestataires de services et, le cas échéant les réviser ou en adopter de nouveaux. Établir un plan d'action afin d'identifier les intervenants et définir leurs rôles et responsabilités quant à la gestion d'un incident de confidentialité. Former et sensibiliser l'ensemble du personnel quant à la sécurité des RP et quant à leur rôle en cas d'incident de confidentialité.

12. COMMISSION D'ACCÈS À L'INFORMATION, *Avis à la Commission d'accès à l'information concernant un incident de confidentialité impliquant des renseignements personnels et qui présente un risque de préjudice sérieux*. Voir notamment : CONSEIL INTERPROFESSIONNEL DU QUÉBEC, *Loi 25 – Guide d'accompagnement pour les ordres professionnels*, Juin 2022.
13 Pour avoir une idée des éléments devant être contenus dans l'avis aux personnes concernées, voir notamment le *Règlement sur les incidents de confidentialité* (articles 5 et 6).

## Gouvernance, Évaluation des facteurs relatifs à la vie privée, Contrat de service : quelques-unes des exigences qui entrent en vigueur en 2023

La *Loi 25* prévoit que toute entreprise « 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 ces renseignements » (art. 3.2). Ce cadre doit préciser le rôle et les responsabilités des membres d'une organisation tout au long du cycle de vie des RP, les modalités applicables à la conservation et à la destruction des RP, ou encore le processus de traitement des plaintes relatives à la PRP. Il doit également être rendu accessible aux clients d'une organisation (art. 3.2).

Elle prévoit également que tout projet d'acquisition, de développement et de refonte de système d'information ou de prestation électronique de services impliquant des RP (art. 3.3) ou encore que toute communication de RP à l'extérieur du Québec (art. 17) doit faire l'objet d'une **évaluation de facteurs relatifs à la vie privée**[14] (« **EFVP** »).

Elle prévoit aussi que le traitement de RP par un fournisseur externe doit faire l'objet d'un **contrat de services** indiquant les mesures à prendre pour assurer la protection du caractère confidentiel du RP communiqué ou encore les obligations en matière d'incident de confidentialité (art. 18.3). Attention, cette dernière exigence ne s'applique pas lorsque le fournisseur est un organisme public au sens de la *Loi sur l'accès* ou un membre d'un ordre professionnel (art. 18.3 al. 3).

## Portabilité : seule exigence qui entre en vigueur en 2024

La *Loi 25* prévoit qu'un RP informatisé recueilli auprès du requérant, et non pas créé ou inféré à partir d'un RP le concernant, pourra lui être communiqué dans un format technologique structuré et couramment utilisé si ce dernier le demande, ainsi que le communiquer à toute personne ou à tout organisme autorisé par la loi à recueillir un tel renseignement (art. 27).

## En guise de conclusion

Comme mentionné, plusieurs dispositions de la *Loi 25* sont en vigueur ou le seront prochainement, il est important de les prendre en considération et ce, même si le projet de loi 3, *Loi sur les renseignements de santé et de services sociaux et modifiant diverses dispositions législatives* est actuellement à l'étude notamment car plusieurs exigences de la *Loi 25* sont reprises dans ce projet de loi : responsable de la PRP, incident de confidentialité, EFVP, consentement et information des personnes concernées, règles de gouvernance et amende en cas de manquement.

### Actions :

Faire un inventaire des renseignements détenus par l'organisation ou qui ont été confiés à un tiers. Procéder à un inventaire des politiques, procédures et pratiques en place, mais aussi des contrats en vigueur pour s'assurer que ceux-ci répondent aux exigences de la *Loi 25*. Revoir les clauses de consentement et les informations communiquées aux clients, incluant les contrats de services professionnels, la politique de confidentialité. Réviser les contrats avec les fournisseurs de services. Mettre en place une procédure en lien avec les EFVP à réaliser. Répertorier les technologies utilisées pour informer les personnes concernées des moyens offerts pour activer les fonctions d'identification, de localisation ou de profilage ou encore pour s'assurer que les paramètres de confidentialité des produits ou services technologiques offerts au public assurent, par défaut, le plus haut niveau de confidentialité. Mettre en place des processus pour la dépersonnalisation et l'anonymisation des RP.

14 COMMISSION D'ACCÈS À L'INFORMATION, *Guide d'accompagnement : Réaliser une évaluation des facteurs relatifs à la vie privée*, 2021 (en révision).