LOI 25

Loi modernisant des dispositions législatives en matière de protection des renseignements personnels

Guide pour les organismes communautaires autonomes

troc cqm
pour un milieu communautaire uni et fort

LA LOI 25

La Loi modernisant des dispositions législatives en matière de protection des renseignements personnels va apporter des modifications importantes aux lois sur la protection des renseignements personnels.

Elle s'applique au secteur privé y compris les OSBL et les organismes communautaires.

Cette loi a pour objectif d'offrir un meilleur contrôle aux citoyens sur leurs renseignements personnels. Elle modernise le cadre législatif pour l'adapter à la réalité technologique d'aujourd'hui.

Sanctionnée en septembre 2021, cette loi entrera graduellement en vigueur, soit en trois phases. Ainsi, certaines dispositions entreront en vigueur le 22 septembre 2022, d'autres le 22 septembre 2023, puis les dernières le 22 septembre 2024.

Cette loi confère des pouvoirs importants à la Commission d'accès à l'information et les mesures correctives peuvent être de nature financière.

UN RENSEIGNEMENT PERSONNEL, C'EST QUOI?

Les renseignements personnels sont ceux qui portent sur une personne physique et permettent de l'identifier. Ils sont confidentiels. Sauf exception, ils ne peuvent être communiqués sans le consentement de la personne concernée.

C'est quoi la protection des renseignements?

Une entreprise qui recueille, utilise, communique à des tiers, conserve ou détruit des renseignements personnels a plusieurs obligations à respecter en vertu de la Loi sur la protection des renseignements personnels dans le secteur privé (Loi sur le privé).

Cycle de vie d'un renseignement personnel

QUELQUES INFORMATIONS SUR LA COLLECTE DES RENSEIGNEMENTS

Des obligations à respecter

Déterminer les fins de la collecte : un intérêt sérieux et légitime doit motiver la constitution d'un dossier sur une personne;

Limiter la collecte de renseignements personnels : la collecte doit se limiter aux renseignements nécessaires aux fins déterminées. En cas de doute, un renseignement personnel est réputé non nécessaire;

Recueillir les renseignements personnels par des moyens légaux et légitimes : sauf exception, la collecte doit se faire auprès de la personne concernée;

Informer la personne concernée, avant de constituer un dossier :

- de l'objet du dossier;
- de l'utilisation qui sera faite des renseignements personnels;
- des catégories de personnes qui y auront accès au sein de l'entreprise;
- de l'endroit où ils seront détenus;
- de ses droits d'accès et de rectification.

Obtenir le consentement des personnes concernées avant de collecter leurs renseignements personnels auprès d'un tiers, à moins d'une exception prévue par la loi.

Quelques exemples de renseignements personnels:

- nom
- âge
- origine ethnique
- adresse civique
- numéro de téléphone
- adresse courriel
- niveau d'éducation
- données biométriques
- dossiers médicaux (informations sur la santé)
- relevés fiscaux
- numéro d'assurance sociale (NAS)
- le contenu de recherches en ligne
- adresse IP
- relevés de compte du téléphone cellulaire utilisé pour son travail
- Autres numéros d'identification

CONSERVATION ET DESTRUCTION

les obligations

Conservation

La conservation est la période durant laquelle un organisme garde des renseignements personnels, sous quelque forme que ce soit, et ce, peu importe que les renseignements soient activement utilisés ou non.

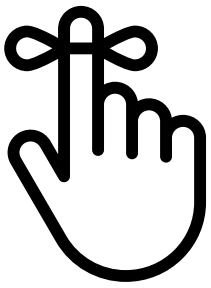
À cette étape, on doit respecter les obligations suivantes :

- **Assurer la qualité des renseignements personnels** en veillant 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;

- **Prendre des mesures de sécurité propres à assurer la sécurité des renseignements personnels**.

Destruction

Le cycle de vie du renseignement personnel se termine lors de sa destruction.



À cette étape, on doit :

Détruire les renseignements personnels de manière sécuritaire dès que la finalité pour laquelle ils ont été collectés est accomplie, sous réserve du délai prévu par la loi ou par un calendrier de conservation établi par règlement du gouvernement (ex. pour des obligations fiscales).

AUTRES OBLIGATIONS

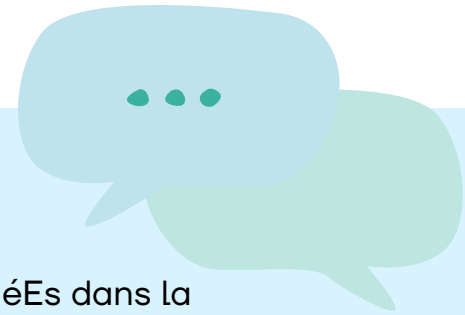
sécurité, accès et rectification

Mettre en place des mesures de sécurité propres à assurer la protection des renseignements personnels collectés, utilisés, communiqués, conservés ou détruits.

- Ces mesures sont raisonnables compte tenu, notamment, de la sensibilité, de la finalité, de la quantité, de la répartition et du support des renseignements personnels.

Permettre l'exercice des droits d'accès et de rectification et répondre avec diligence, dans les 30 jours, aux demandes d'accès aux renseignements personnels et de rectification soumises par les personnes concernées.

- L'absence de réponse dans ce délai équivaut à un refus. Un citoyen peut contester un refus ou une réponse jugée insatisfaisante en exerçant son droit de recours devant la Commission d'accès à l'information.



Des bonnes pratiques :

- Préciser les rôles et obligations des employéEs impliquéEs dans la protection des reinseignements personnels (RP);
- Tenir à jour un inventaire de RP détenus par l'organisme;
- Rédiger un consentement à **faire remplir systématiquement et signer** par les personnes collectées
- Faire rapidement le traitement de demandes et/ou plaintes
- En cas de changement de système informatique s'assurer de respecter la Loi

CALENDRIER

Des nouvelles obligations

dates	Nouvelles obligations
Septembre 2022	• Désignation d'un responsable de la protection des renseignements personnels. Son titre et ses coordonnées doivent être disponibles sur le site internet • Notification et consignation des incidents de confidentialité* prendre les mesures pour éviter que cela n'arrive plus et aviser la Commission d'accès à l'information et la personne concernée • Tenir un registre d'incidents
Septembre 2023	• Adopter ou mettre à jour des politiques et des pratiques encadrant la gouvernance des renseignements personnels (établir votre **politique et pratiques pour la gestion** de RP et la publier sur votre site internet) • Réalisation d'Évaluations de Facteurs relatifs à la Vie Privée (EFVP) pour certains traitements de renseignements personnels. Guide pour réaliser une EFVP • **Détruire** les RP quand la finalité est accomplie ou les **anonymiser** • obtenir au préalable**, le consentement de la personne** pour utiliser ses renseignements personnelles à des fins de statistique ou autres • Respecter les nouvelles règles pour le consentement à la collecte et l'utilisation des RP

dates (suite)	Nouvelles obligations
Septembre 2024	• Communiquer, à la demande de la personne concernée, ses renseignements personnels fournis au préalable à l'organisme • Répondre aux demandes de **portabilité (communiquer un RP informatisée accessible à la personne concernée).** Informer son webmestre que dorénavant le système informatique devra pouvoir fournir un RP informatisé aux participantEs ou à un organisme autorisé par la Loi à recueillir le renseignement, à la demande de la personne.

Incidents de confidentialité:

Qu'est-ce qu'un incident de confidentialité?*
Pour l'application des lois, un incident de confidentialité correspond à tout accès, utilisation ou communication non autorisés par la loi d'un renseignement personnel, de même qu'à la perte d'un renseignement personnel ou à toute autre atteinte à sa protection.

Par exemple, un incident de confidentialité pourrait se produire lorsque :

- un membre du personnel consulte un renseignement personnel sans autorisation;
- un membre du personnel communique des renseignements personnels au mauvais destinataire;
- l'organisation est victime d'une cyberattaque : hameçonnage, rançongiciel, etc.

Si une organisation a des motifs de croire qu'un incident de confidentialité impliquant un renseignement personnel qu'elle détient s'est produit, elle doit prendre les mesures raisonnables pour diminuer les risques qu'un préjudice soit causé et éviter que de nouveaux incidents de même nature ne se produisent.

un avis d'incident doit comprendre:

- Les circonstances
- La date ou la période ou il y a eu lieu
- La nature des RP visés
- Les mesures prises par l'organisation et par tout intéressé afin de réduire le risque de préjudice qui pourrait en résulter
- Les coordonnées permettant à la personne intéressée de se renseigner d'avantage sur l'incident

PLUS CONCRÉTEMENT

dans la vie de tous les jours de votre organisme

- Posez-vous la question : " est-ce que mon organisme à **vraiment besoin de toutes les informations demandés** lors de l'adhésion de mes membres ?

- Créer une **politique** à l'interne pour la protection des renseignements personnels

- Expliquez à vos membres (ou toute personne qui vous fournit de RP) que vous avez besoin de **leur consentement écrit** pour récolter les informations demandées

- **Créer** et **faire signer** le dit consentement dans un papier distinct

- Expliquez clairement à vos membres que votre organisme à une **préoccupation constante** relative à préserver leur confidentialité

- Afficher sur votre site internet le **nom** et les **coordonnées** de la **personne responsable** de la conservation des renseignements personnels

- Réviser et/ou revoir votre base de données s'il y a lieu (ou l'endroit où vous conservez les RP)

- **Détruire** ou **anonymiser** les informations qui ne vous sont plus utiles

- Créer un mécanisme de fonctionnement pour le **traitement des plaintes** et la **déclaration des incidents**

AUTRES RESSOURCES ET LIENS

- 📌 Un document foire aux questions sur la protection des renseignements personnels dans le secteur privé, du Réseau québécois des OSBL en habitation : https://bit.ly/40EQAfF

- 📌 L'aide-mémoire sur les nouvelles responsabilités des entreprises, les pistes d'action et les bonnes pratiques de la commission d'accès à l'information du Québec : https://www.cai.gouv.qc.ca/entreprises/

- 📌 Présentation, RQ- ACA sur la Loi 25 : https://bit.ly/3HNz6b1

- 📌 Tableau avec les échéanciers et comparant la loi actuelle et les changements à venir : https://bit.ly/3jkcQeE

- 📌 Loi sur la protection des renseignements personnels dans le secteur privé : https://bit.ly/448jfww

- 📌 Guide d'accompagnement pour réaliser une évaluation des facteurs relatifs à la vie privée de la commission des d'accès à l'information : Guide pour réaliser une EFVP

- 📌Exemple de politique de confidentialité partagé par le Réseau d'aide le Tremplin : https://bit.ly/3olTpiG

- 📌 Un modèle de registre d'incident de confidentialité : Registre d'incident

- 📌 À nouveau le document produit par Me Andréanne Lascelle-Lavallée du CJP Mauricie sur la Loi 25 : CJP Mauricie Loi 25