

# Loi sur la protection des renseignements personnels

(dans le secteur privé)

Résumé

Loi 25



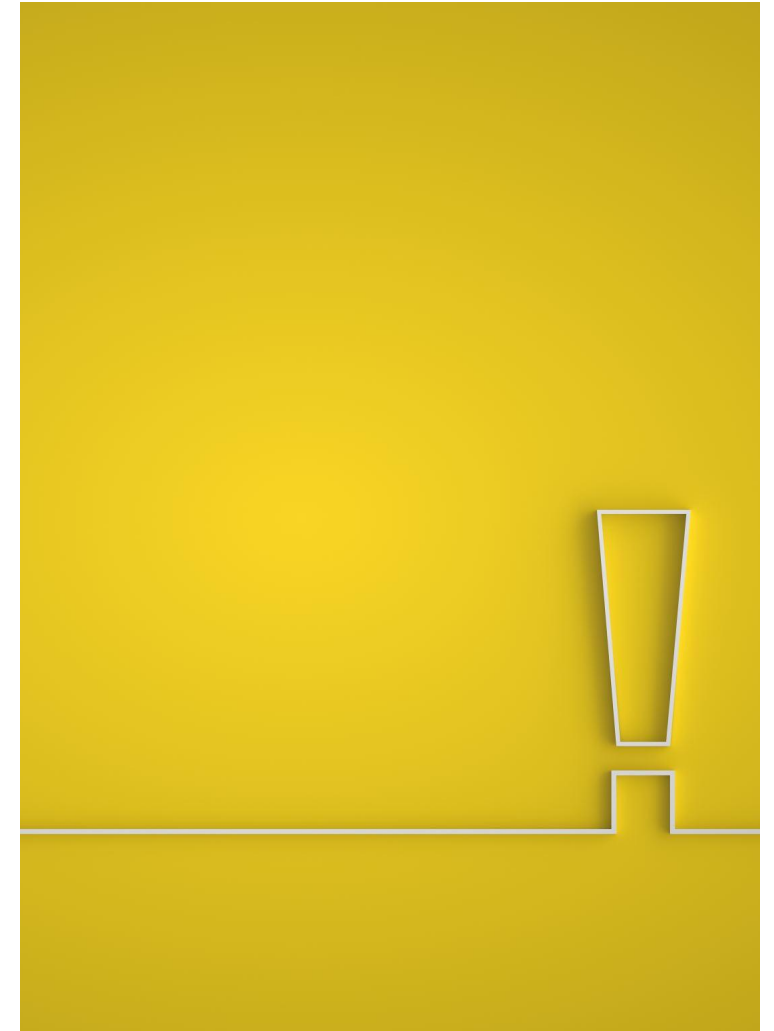
cradi

COMITÉ RÉGIONAL POUR L'AUTISME  
ET LA DÉFICIENCE INTELLECTUELLE



# Mise en application (3 dates à retenir)

- 22 septembre 2022 : oui, c'était l'an dernier !
  - nomination du responsable et publication
  - Registre des incidents
  - Aviser si incident de confidentialité
- 22 septembre 2023 : présentation disponible le 19 septembre
  - Cadre et politique et publication
  - Consentement et aviser la personne concernée (but/conservation/utilisation)
  - Liste des renseignements personnels collectés et ÉFVP
- 22 septembre 2024 : remettre (document numérisé) sur demande de la personne concernée tout renseignement récolté sur elle.



# APPLICATION ET INTERPRÉTATION



## **Objet de la Loi (art 1)**

Établir des règles particulières à l'égard de tout renseignement personnel sur autrui qu'une personne recueille, détient, utilise ou communique à des tiers dans l'exploitation d'une entreprise ou d'un organisme dans notre cas.

# APPLICATION ET INTERPRÉTATION



## Définition de renseignement personnel (art. 2)

Est un renseignement personnel, tout renseignement qui concerne une personne physique et permet de l'identifier. Ils sont confidentiels. Ils ne peuvent être communiqués sans consentement.

- *Personne physique : employé, bénévole, membre, membre du Conseil d'administration, participant et usager à des activités ou des services, etc.*
- *Renseignements personnels directs (nom complet, NAS, permis de conduire, courriel, etc.) ou indirects (doivent être combiné : CP, sexe, nationalité, profession, état civil, préférences de..., etc.)*
- *Renseignement public*
  - *Renseignement personnel utilisé professionnellement (ex : courriel)*
- *Renseignement sensible*

**RESPONSABILITÉ : qui?**

**OBLIGATIONS : de quoi?**



**Obligation générale : respecter les règles en matière de consentement à la collecte, à la conservation, à la protection et à l'utilisation des renseignements personnels.**

- a. Pour la protection (politique, responsable, bonne pratique, etc.)
- b. Lors d'un incident
- c. Lors de la Collecte (but spécifique, nécessité, etc.)
- d. Quant au caractère confidentiel (conservation, protection, destruction, etc.)
- e. Lors d'une transmission sans consentement (très rare)
- f. Lors d'une demande de la personne concernée
  - demande d'accès
  - de modification/ rectification
  - de retrait de consentement

# RESPONSABILITÉS ET OBLIGATIONS

## Responsabilités (art 3.1)

Est responsable de la protection des renseignements personnels toute personne qui exploite une entreprise :

Généralement, la plus haute autorité (donc la présidence du CA)

— Peut déléguer (Devrait) (**obligations d'un OC : nommer un responsable de la protection des renseignements personnels et établir les rôles. Devait être fait avant le 22 septembre 2022.**)

À qui ? DG, DGA, Coordo. (Autorité suffisante)

Par écrit (*résolution claire*)

*96. Une association ou une société qui exploite une entreprise et détient des renseignements personnels sur ses membres ou sur des tiers **a les mêmes droits et les mêmes obligations à l'égard de ses membres et des tiers que la personne qui exploite une entreprise (présidence du CA demeure responsable)***

Nom et titre de la personne responsable **doivent être publiés (avant le 22 septembre 2022)**

Site Internet (dans contact; voir message type)

Tout autre moyen approprié (infolettre, Facebook ou autres, à ajouter à la signature de courriel du/de la responsable par exemple)



# RESPONSABILITÉS ET OBLIGATIONS

---

## Obligations (quant à la protection générale)

**Obligation** : Établir des politiques et pratiques (pour la transparence) encadrant sa gouvernance à l'égard des renseignements personnels détenus et utilisés (art 3.2), par une **politique de gestion et protection des renseignements personnels** (art 8.2) : voir modèle du CRADI

-concernant la pratique de la collecte à la destruction (la conservation, les rôles et responsabilités du personnel (le CA, le responsable et toute personne susceptible de récolter des données personnelles), le processus de traitement des plaintes, de modification de consentement, la procédure d'accès, de modification ou destruction, etc.

Être approuvé (avec résolution du CA) et signé par le responsable

Publier (et accessible facilement)



# RESPONSABILITÉS ET OBLIGATIONS



## Obligations (quant à la protection...suite)

Faire une liste des données personnelles collectées ou à collecter (à inclure dans la Politique)

**Obligation :** Compléter une évaluation des facteurs à la vie privée – ÉFVP :

Pour chaque projet (ex : REQ) (art 3.3), même s'il n'y aura pas communication à des tiers (**bonne pratique**)

Avant de partager des données personnelles sans consentement (voir art 18 à 21.0.2). **Donc, faites signer des consentements.**

*Le responsable peut appliquer des mesures additionnelles de protection (mais, en principe, ça sera toujours fait par le responsable)*

Voir formulaires types (liste, ÉFVP et consentement)

**ÉFVP (art 3.7) :**

Dans notre évaluation, on doit considérer la **sensibilité** du renseignement concerné, les conséquences appréhendées de son utilisation et la probabilité qu'il soit utilisé à des fins préjudiciables.

# RESPONSABILITÉS ET OBLIGATIONS



## Le consentement

Le consentement doit être manifeste et expresse (ne pas être implicite, on ne peut le présumer, pas d'un tiers), libre (sans contrainte), éclairé (et informé) et être donné à des fins spécifiques (ce n'est pas une partie de pêche!) (art 14).

**Obligation** de donner la possibilité de modifier ou retirer ce consentement, sur demande.

Attention si renseignement personnel d'un mineur :  
consentement des parents. Pensez à la loi sur la Curatelle, etc.

Et autres lois.

# RESPONSABILITÉS ET OBLIGATIONS (SI...)



## Si incident de confidentialité (art 3.5) : Obligations

*Définition « incident de confidentialité » (art 3.6)*

- *Accès non autorisé à un renseignement personnel*
- *Utilisation non autorisée d'un renseignement personnel*
- *Communication non autorisée d'un renseignement personnel*
- *Perte d'un renseignement personnel ou toute autre atteinte à la protection d'un tel renseignement (cyberattaque, vol, rançongiciel, etc.)*

**Prendre des mesures** pour réduire les risques et ne pas les répéter.

Si pourrait causer un dommage sérieux, **aviser rapidement la Commission d'accès à l'information et la personne** dont un renseignement personnel est concerné par l'incident. Peut être contraint de le faire par la Commission. C'est une obligation!

**Maintenir un registre** (voir modèle) **et inscrire l'incident**. Le rendre disponible à la Commission sur demande (art 3.8). Fournir à la Commission de toutes infos supplémentaires

**Aviser** toute personne ou tout organisme susceptible de diminuer ce risque.

# RESPONSABILITÉS ET OBLIGATIONS

---

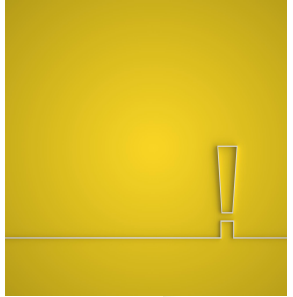


POUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET ÉVITER LES INCIDENTS, NE PARTAGEZ PAS DE RENSEIGNEMENTS PERSONNELS SANS CONSENTEMENT. ASSUREZ-VOUS D'AVOIR LES CONSENTEMENTS APPROPRIÉS.



VAUT MIEUX PROAGIR POUR NE PAS À DEVOIR RÉPARER DE POTS CASSÉS !

# OBLIGATIONS ET PRATIQUES POUR LA COLLECTE DES DONNÉES PERSONNELLES



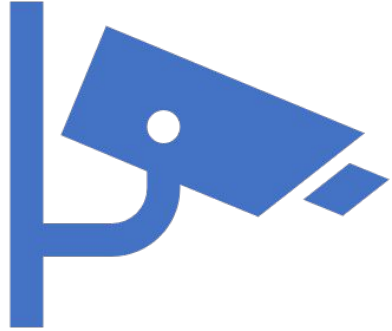
**Objet** - toujours se demander pourquoi on collecte (art 4) : emploi, activités, REQ, etc. Ça aide à déterminer les risques et la nécessité de collecter.

Uniquement **ce qui est nécessaire** à l'objet (art 5). En cas de doute, c'est jugé non nécessaire (art 9). En passant, le NAS n'est obligatoire qu'après l'embauche.

Auprès de la **personne même**, sauf si consentement de recueillir d'un tiers (art 6)

Source du renseignement personnel, le cas échéant (art 7)

**Obligation** : d'informer la personne de qui on collecte de la raison spécifique, l'utilisation, la conservation, la durée, la politique, l'accès, etc., lors de la collecte.



## CARACTÈRE CONFIDENTIEL DES RENSEIGNEMENTS PERSONNELS

---

Prendre des mesures raisonnables de sécurité appropriée (art 10) : conservation

Données à jour et exactes avant de les utiliser ou les partager (art 11) : utilisation

Utilisation permise après fin de l'objet qu'avec consentement (art 12) (ex : changement au CA)

Aucune utilisation à des fins non-pertinentes sauf consentement (art 13)

# Obligations lors de communication **sans consentement** à des tiers



Sans le consentement, principalement si acte criminel, si convention collective, si une vie est en danger, si nécessaire pour un projet, transaction ou un contrat, etc. (art 18 à 18.3). Doit être inscrit dans le dossier ou dans le registre d'incident.

Sans le consentement, si recherche, études ou production statistiques, et si ÉFRV conclut que c'est OK. (art 21).

Demande par écrit et détails (art 21.0.1).

Entente entre la personne responsable et la personne qui demande l'information (art 21.0.2).

# DEMANDE D'ACCÈS ET AUTRES RESPONSABILITÉS (lors de demande)



## Dispositions générales

**Dans les 30 jours de la date de réception.** Sinon, c'est considéré comme un refus (art 32)

Demande d'accès par écrit (avec pièce justificative le cas échéant) : si personne handicapée, mesures d'accommodement raisonnable. Prendre mesures nécessaires pour que l'accès soit libre (art 29)

Correction/ modification/ retrait

Accès gratuit, sauf si frais raisonnables (art 33)

Refus avec motif et avis (art 34) : et processus de traitement de plainte...

Si demande de rectification acceptée, envoi d'une copie (art 35). + art 40 CCQ.

Si demande refusée, obligation de conserver le renseignement jusqu'à procédures judiciaires finales (art 36).

# Traitement des plaintes (interne)



- Pour toute mécontente sur l'application de la Loi
- Pour toute demande refusée (ou silence) : simple

Procédures pour une rencontre et discussion

S'il n'y a pas de règlement entre les parties, la personne concernée pourra faire une demande à la Commission.

# 10 règles ou obligations à suivre

Respecter les règles (Lois, politiques)

Nommer un responsable, établir des Politiques et publier (À FAIRE)

Effectuer des Évaluation des Facteurs de la Vie Privée ÉFVP (À FAIRE)

Lors de la collecte : nécessité, informer, consentement

Lors de la conservation : sécuritaire

Lors de l'utilisation : consentement, exactitude, précision

Donner accès et répondre aux demandes dans les 30 jours

Si incident (réduire le risque, aviser, registre)

Régler les mécontentes

NE PARTAGEZ PAS SANS CONSENTEMENT !

# LES RECOURS ET PÉNALITÉS

Devant la Commission d'accès à l'information (art 54 à 60)

Pénalités administratives et pénales

- administratives : plusieurs millions de \$
- pénales : plusieurs dizaines de milliers de \$

---

## Pour terminer...

Possibilité d'être inspecté : et le mandat de l'inspecteur est large.

Possibilité d'être enquêté par la Commission : à la suite d'une plainte ou de leur propre initiative

Donc, assurez-vous d'être à jour !



# Autres références utiles

---

- Pour consulter le texte de Loi : [P-39.1 - Loi sur la protection des renseignements personnels dans le secteur privé \(gouv.qc.ca\)](#)
- Pour consulter la boîte à outils du RIOCM sur la Loi 25 : [Loi 25 : Protection des renseignements personnels - RIOCM](#)
- Pour consulter le guide de la Commission d'accès à l'information : [Vers la conformité à la loi sur le privé : Nouvelles responsabilités et obligations des entreprises | CAI](#)
- Pour réaliser une évaluation des facteurs relatifs à la vie privée, c'est-à-dire une démarche préventive visant à mieux protéger les renseignements personnels et à mieux respecter la vie privée des personnes physiques : [Guide d'accompagnement - Réaliser une évaluation des facteurs relatifs à la vie privée.](#)
- Commission d'accès à l'information : <https://www.cai.gouv.qc.ca/>



Questions  
([direction@cradi.com](mailto:direction@cradi.com))