LOI 25

PLAN D'ACTION

LOI 25 - COMMENT L'APPLIQUER?

PROTECTION VIE PRIVÉ

PAR MÉLISSA DALLI CARDILLO - ADN

La Loi 25 a pour objectif de moderniser les dispositions législatives pour la protection des renseignements personnels au Québec, afin qu'elles correspondent mieux aux défis rencontrés aujourd'hui dans un environnement numérique et technologique récent.

Les mesures de cette nouvelle législation entrent en vigueur de façon progressive sur une période de trois ans. Ce guide a pour but de vous accompagner lors de l'implantation de ces changements auprès de votre organisme de loisir. Vous trouverez dans ce guide un plan d'actions concrètes à mettre en place pour respecter les différentes échéances:

- Première échéance : 22 septembre 2022
- Deuxième échéance : 22 septembre 2023
- Troisième échéance : 22 septembre 2024

BULLETIN D'INFORMATION SUR LA LOI 25

SOMMAIRE

ACTIONS SEPTEMBRE 2022

PLAN D'ACTION

☑ NOMMER UN·E RESPONSABLE DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS (RPRP)

Si personne n'est nommé, c'est alors le rôle de la plus haute autorité de l'organisme. Le·la président·e de CA peut déléguer cette responsabilité à un membre de l'équipe pour faire respecter la loi et la mise en œuvre de celle-ci.

☑ RENDRE PUBLIC LE TITRE ET LES COORDONNÉES DU RESPONSABLE SUR LE SITE WEB OU TOUTE AUTRE PLATEFORME

Vous devez publier les coordonnées du RPRP sur votre site web. Si vous ne possédez pas de site web, vous devez publier l'information par tout autre moyen approprié. Il peut s'agir de votre page Facebook. Cette information doit être visible idéalement dans votre politique de confidentialité. Si vous n'en avez pas, vous pouvez rendre cette information disponible sur la page de contact de votre site web.

EXEMPLE DE TEXTE À AJOUTER POUR LES COORDONNÉES DU RPRP:

> *Pour toute question au sujet du traitement ou de la mise à jour de vos renseignements personnels ou pour nous faire part de toute préoccupation à cet égard, veuillez communiquer avec nous par le biais de l'adresse courriel suivante: xxx@nomorganisme.com*.*
> *Le·la responsable de la protection des renseignements personnels prendra contact avec vous dans les trente (30) jours suivant la réception de votre courriel.*

*Vous pouvez créer une adresse courriel générique pour toutes les demandes reliées à la PRP, par exemple viepriveee@nomorganisme.com

☑ METTRE EN PLACE UNE POLITIQUE QUI DÉTAILLE LES RESPONSABILITÉS DU RPRP

Il faut également mettre en place une politique qui va détailler les responsabilités du·de la responsable de la protection des RP. Son rôle et ses responsabilités sont principalement:

- Établir la politique et les pratiques de gouvernance en matière de protection des RP
- Élaborer un processus de traitement des plaintes en matière de RP
- Assurer la gestion des incidents de confidentialité
- Réaliser les Évaluations de Facteurs relatifs à la Vie Privée (ÉFVP)
- Sensibiliser et former le personnel de l'organisme

À noter que ces différentes responsabilités vont être mises en place progressivement avec le changement de législations de la loi 25.

☑ FORMATION DE SENSIBILISATION SUR LA PROTECTION DES RP

Le.a responsable devra mettre en place un programme de formation et de sensibilisation sur la protection des renseignements personnels au sein de l'organisme.

☑ CRÉER ET TENIR UN REGISTRE D'INCIDENTS DE CONFIDENTIALITÉ

Ce registre va répertorier les incidents de confidentialité au sein de votre organisme qui peuvent porter un préjudice sérieux. Un incident de confidentialité est l'accès, l'utilisation, la communication d'un renseignement personnel non autorisés par la loi ou la perte ou tout autre atteinte à la protection. Il est important de mettre en place un processus d'action en cas d'incidents sur la confidentialité, il faudra notamment communiquer les incidents à la Commission d'accès à l'information du Québec.

Consultez l'annexe pour télécharger un exemple de registre d'incidents de confidentialité

☑ FAIRE UN INVENTAIRE DES RENSEIGNEMENTS PERSONNELS DE L'ORGANISME

Un inventaire des RP doit aussi être créer. Il s'agit d'un document répertoriant où et comment les RP sont collectés.

Consultez l'annexe pour télécharger un exemple d'inventaire des renseignements personnels

ACTIONS SEPTEMBRE 2023

PLAN D'ACTION

CRÉATION ET VISIBILITÉ DE LA POLITIQUE DE CONFIDENTIALITÉ

Il faut créer ou mettre à jour une politique de confidentialité concernant les renseignements personnels auxquels votre organisme a accès. Cette politique doit être rendue disponible sur votre site web ou toute autre plateforme. La politique de confidentialité doit au minimum inclure les éléments suivants:

- Coordonnées du·de la responsable de la protection des renseignements personnels
- Liste des RP collectés
- Explication de l'utilisation prévue avec ces renseignements personnels
- Délai de conservation des données
- Conditions d'accès, rectification et retrait

Il n'est jamais facile de rédiger une politique de confidentialité. Vous pouvez consulter un avocat pour créer votre politique ou vous pouvez vous inspirer de ce qui est existant.

COLLECTE DU CONSENTEMENT

Le **consentement** doit être collecté de manière:

- **Manifeste**: de façon certaine,
- **Libre**: sans contrainte,
- **Éclairé**: comprendre pourquoi et
- **Spécifiques**: pour une finalité déterminée

Le consentement peut être collecté de plusieurs façons. Il doit être donné par une déclaration ou tout acte positif clair. Il peut s'agir de case à cocher, de pop-up sur le site web ou tout autre dispositif permettant à l'utilisateur de consentir à l'utilisation de ses données pour une durée et un but déterminé.

METTRE EN PLACE DE PLUSIEURS PROCÉDURES ET PRATIQUES POUR LE CYCLE DE VIE DES DONNÉES

Il y a plusieurs procédures internes à mettre en place relative à la protection des RP, notamment:

LA PROCÉDURE DE CONSERVATION, DE DESTRUCTION ET D'ANONYMISATION DES RP

Les renseignements personnels ont un cycle de vie au sein de votre organisme, il faudra encadrer ce cycle de vie par une procédure de conversation des données.

Cycle de vie RP — Collecte — Utilisation — Communication — Conservation — Destruction

Il faudra répondre aux questions suivantes dans ce procédurier:

- Quels sont les délais de conservation de nos RP?
- Que fait-on lorsque nos RP ont atteint leur durée de vie? Deux options s'offrent à vous: La destruction de TOUTES les copies de la donnée ou l'anonymisation. La deuxième option signifie qu'il n'est plus possible d'identifier directement ou indirectement une personne et ce d'une façon irréversible. L'anonymisation devra être légitime et justifiée.

LA PROCÉDURE DE DEMANDE DE DÉSINDEXATION / DE SUPPRESSION DES RP

Toute personne a le droit de demander que ses données personnelles soient effacées. Il faut cependant examiner la demande car dans certains cas vous ne pouvez pas supprimer les données puisque vous avez des obligations à conserver certains éléments. C'est notamment le cas si vous fournissez des biens ou/et des services à une personne, garder des données dans le cadre d'exigences du droit du travail ou encore pour des raisons juridiques.

ACTIONS SEPTEMBRE 2023

☑ LA PROCÉDURE DE TRAITEMENT DES PLAINTES ET DE DEMANDE D'ACCÈS AUX RP

Toute personne dont vous collecter des données a le droit de demander une copie des renseignements personnels que vous avez sur elle. C'est pourquoi il est utile d'avoir mis en place un inventaire de vos données, ainsi vous savez où la donnée est enregistrée et ce que vous collectez.

⚠ Il est primordial de vérifier l'identité de la personne vous faisant la demande avant de donner les RP et de préciser quel est le délai de traitement pour recevoir une réponse.

Vous devez également mettre en place un processus pour la réception des plaintes concernant la collecte des renseignements personnels et donner suite aux plaintes qui sont recevables.

☑ LA PROCÉDURE DE GESTION DES INCIDENTS DE SÉCURITÉ ET VIOLATIONS DES RP

Il faut mettre en place une procédure claire et précise pour savoir que faire dans le cas d'un incident de sécurité, de confidentialité ou de violation des renseignements personnels.

☑ LA PROCÉDURE DE GESTION DU PERSONNEL

Il faut mettre en place une procédure claire concernant la gestion des accès aux données personnelles au sein de votre organisme. Il est important de limiter les accès aux personnes qui en ont vraiment besoin et d'enlever les accès aux personnes quittant votre organisme.

📎 *Consultez l'annexe pour télécharger un exemple de fichier pour gérer les rôles et les accès du personnel*

☑ ÉVALUATION DE FACTEURS RELATIFS À LA VIE PRIVÉE (EFVP)

Cette évaluation doit être réalisée à chaque nouveau projet d'acquisition, de développement ou de refonte de système d'information ou de prestation électronique de services qui implique la collecte, l'utilisation, la communication ou la destruction des renseignements personnels OU lors d'un transfert/ de communication de renseignements personnels à l'extérieur du Québec.

📎 *Consultez l'annexe pour télécharger un exemple de liste de comptes pour déterminer quelles sont les informations sensibles sur toutes les plateformes que vous utilisez*

PLUS D'INFORMATION POUR 2023

La Commission d'accès à l'information du Québec étudie encore comment mettre en place certaines mesures pour septembre 2023. Des nouvelles directives et éclaircissements de loi devraient être communiqués par la Commission.

ACTIONS SEPTEMBRE 2024

PLAN D'ACTION

DROIT À LA PORTABILITÉ DES RP

Une personne peut demander que les renseignements personnels recueillis à son sujet lui soient communiqués ou soient communiqués à une autre organisation dans un format déterminé.

13 MESURES DE CONTRÔLE DU CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

1. Élaborer un plan d'intervention en cas d'incident: mettre en place un procédurier dans le cadre d'une cyber attaque (quoi faire, comment agir, et que faire après).
2. Appliquer des correctifs aux applications et aux systèmes d'exploitation:
   a. Améliorer la sécurité et protection actuelle de vos plateformes
   b. Consultez l'inventaire des renseignements personnels pour améliorer la protection de vos données.
3. Utiliser une authentification forte: il existe plusieurs façon de s'assurer d'avoir un mot de passe fort, notamment la création de mot de passe fort (18 caractères, utiliser une phrase et prendre la première lettre de chaque mot, l'identification à double facteur) ou encore utiliser un gestionnaire de mots de passe.
4. Sauvegarder et chiffrer les données: il est important de savoir sur quel dispositif les sauvegardes sont faites (serveurs, ordinateur, stockage infonuagique, etc.) et combien de copie de vos données vous avez.
   Petit conseil: Faire plus d'une sauvegarde de vos données avec la règle de 3 copies sur 2 supports et 1 hors site.
5. Activer les logiciels de sécurité
6. Former les employés
7. Sécuriser les services infonuagiques et les services de TI externalisés
8. Sécuriser les sites web
9. Mettre en œuvre des contrôles d'accès et d'autorisation
10. Sécuriser les dispositifs mobiles
11. Configurer les dispositifs pour assurer leur sécurité
12. Établir un périmètre de défense de base
13. Sécuriser les supports amovibles

PLUS D'INFORMATION POUR 2024

La Commission d'accès à l'information du Québec étudie encore comment mettre en place certaines mesures pour septembre 2024. Des nouvelles directives et éclaircissements de loi devraient être communiqués par la Commission.

DÉFINITIONS & ANNEXES

DÉFINITIONS

PRÉJUDICE SÉRIEUX

Un préjudice sérieux est une atteinte à la réputation, au dossier de crédit, une perte financière ou perte d'emploi ou un vol d'identité.

RENSEIGNEMENTS PERSONNELS

Les renseignements personnels sont ceux qui portent sur une **personne physique** et permettent de **l'identifier**. Ils sont confidentiels. Sauf exceptions, ils ne peuvent être communiqués sans le **consentement** de la personne concernée. Ce qui signifie qu'un renseignement professionnel n'est pas un renseignement personnel. Ce n'est pas une raison pour ignorer la protection des données professionnelles car il en vient à votre réputation. Voici quelques exemples de données personnelles:

Nom et prénom	Adresse courriel	Langues parlées
Date de naissance	Adresse IP	Niveau d'éducation
Adresse postale	Géolocalisation	Habitudes de consommation
Numéro de téléphone	Situation familiale	Numéro de membre
Numéro de carte de crédit	Nationalité	...
Numéro d'assurance sociale	Renseignements financiers	
Numéro de passeport	Renseignements médicaux	

ANNEXES

EXEMPLE REGISTRE D'INCIDENT DE CONFIDENTIALITÉ

Comme mentionné, il faut tenir un registre d'incidents de confidentialité **ET** vous avez pour obligation de communiquer les incidents de confidentialité à la commission d'accès à l'information du Québec.
Vous pouvez télécharger le gabarit de la loi 25 ici et consulter la page "Registre d'incidents de conf.".

EXEMPLE D'INVENTAIRE DES RENSEIGNEMENTS PERSONNELS

Vous pouvez consulter la page "Inventaire RP" dans le même gabarit Excel ou le retélécharger ici.
Il y a plusieurs étapes à réaliser concernant l'inventaire des renseignements personnels.

1. Faire l'inventaire des renseignements personnels que vous possédez.
2. Évaluer le degré de sensibilité de vos renseignements personnels
3. Déterminer les lieux où sont conservés ces RP
4. Requestionner la collecte de ces RP
5. Déterminer qui a accès à ces RP
6. Identifier les mesures de sécurité des applications et logiciels où sont conservés ces RP

EXEMPLE DE LISTE DE COMPTES

Pour vous aider à déterminer les lieux où sont conservés vos données, vous pouvez consultez la page "liste de comptes" dans le même gabarit Excel ou le retélécharger ici.

EXEMPLE DE LISTE POUR GÉRER LES RÔLES ET LES ACCÈS DU PERSONNEL

Pour vous aider à déterminer qui a accès aux renseignements personnels, vous pouvez consultez la page "Liste des rôles et des accès" dans le même gabarit Excel ou le retélécharger ici.

SOURCES

- Formation 7 décembre donnée par Emeline Manson, "Loi 25 - Par où commencer?", formatrice experte en prévention des fraudes et en cybersécurité de cy-clic.com. Les gabarits sont offerts par la formatrice Emeline Manson.
- Commission d'accès à l'information, "Loi 25 - Nouvelles dispositions protégeant la vie privée des Québécois - Certaines dispositions entrent en vigueur aujourd'hui", www.quebec.ca, 22 septembre 2022, lien
- Commission d'accès à l'information, "Vers la conformité à la Loi sur le privé", cai.gouv.qc.ca, 16 septembre 2022, lien