Mis à jour le 16 novembre 2023

ROCLD – Guide d'accompagnement Loi 25

Rédigé par Simon Beaudin, analyste sociopolitique

Le présent guide se veut un outil d'accompagnement dans la mise en conformité avec la loi 25, produit par le ROCLD et destiné à ses membres. Le guide est complémentaire et organisé de la même manière que les 4 rencontres de soutien qui se tiendront à l'automne 2023. Notre objectif est de fournir une information synthétisée relativement à la loi 25 et d'offrir une marche à suivre simple et structurée vers son application.

Vous trouverez tout au long du document des hyperliens menant à des outils (formulaires, modèles, etc.), dont plusieurs développés par la Coalition Interjeunes. Vous retrouverez également ceux-ci rassemblés en fin de documents.

TABLE DES MATIÈRES

BLOC 3

BLOC 4

BLOC 1

1. La mise en conformité à la loi 25

Qui doit se conformer à la loi 25?

- Toutes les organisations qui ont un numéro d'entreprise doivent se conformer.

À partir de quand la loi s'applique-t-elle?

- La très grande majorité des dispositions de la loi 25 s'appliquent déjà (depuis les 22 septembre 2022 et 2023). Le droit à la portabilité va s'ajouter dans les nouvelles obligations à partir du 22 septembre 2024.

Audit informatique

- Le gouvernement vérifier l'application de la loi 25 au moyen d'audits informatiques. Ceux-ci vont être réalisés à la pige ou à la suite d'une plainte.
- Lors d'un audit informatique, des agents viennent sur place et vérifient l'ensemble du parc informatique de l'organisation.

Pénalité de non-conformité

- Les pénalités varient de 500$ à 6% des revenus de l'organisation.

Assurances et cybersécurité

- Il est important de vérifier auprès de vos assurances pour vous protéger en cas de litige impliquant des RP. Plusieurs assureurs sont en train de retirer les protections concernant la cybersécurité.

Mise en conformité et gestion du risque

- L'ensemble du Québec se met à jour quant aux nouvelles obligations de la loi. Le gouvernement n'a pas les ressources pour auditer l'ensemble des organisations sur son territoire. Il est important de se conformer à la loi 25, mais même si vous avez du retard dans l'application de la loi, les chances demeurent minces pour que vous viviez un audit informatique rapidement.

Mise en conformité et ressources externes

- Dans un monde idéal, allez chercher un accompagnement externe. D'une part, auprès d'une firme en sécurité informatique. D'autre part, si des questions d'ordre légales ressortent de vos travaux, auprès d'un.e avocat.e qualifié.e en la matière.
- Pour tout besoin à ce sujet vous pouvez me rejoindre : analyste@rocld.org

2. Définition des concepts

Renseignements personnels (GVC – webinaire)

- Les renseignements personnels (RP) sont par défaut des renseignements confidentiels.
- Un RP est un renseignement qui permet d'identifier une personne physique.
- Un renseignement devient un RP lorsqu'il est combiné à d'autres renseignements. Par exemple, le nom et prénom ne sont pas des RP par eux-mêmes. S'ils s'accompagnent d'un autre renseignement (ex. adresse, téléphone, etc.) ils deviennent des RP.

Types de RP

Nom	Information de santé
Prénom	Notes évolutives
Courriel	Orientation sexuelle
Téléphone	Identité de genre
Adresse	Convictions religieuses
Date de naissance	Pays d'origine
Numéro d'assurance sociale	Statut d'immigration
Carte de crédit	État civil
Permis de conduire	

RP selon différents types de documents

Courriel	La loi 25 s'y applique s'il contient le nom de la personne ou d'autres RP. Solution si on ne veut pas détenir ces RP : on répond et on supprime rapidement le courriel (supprimer, vider la corbeille et vérifier qu'il n'y a pas de sauvegarde.
Clavardage (chat)	La loi 25 s'y applique s'il contient des RP.
CV	La loi 25 s'y applique.
Réseaux sociaux	Il n'y a pas d'informations à proprement dit dans la loi 25. Si des RP se retrouvent sur votre page ou une de vos publications (par exemple en commentaire), on devrait les considérer comme des RP.
Liste de présence à un atelier	Ce n'est pas un RP si on y trouve seulement le nom, prénom et la présence de la personne. La loi 25 s'y applique si on y retrouve davantage de RP.
Photos et vidéos	La loi 25 n'a pas statué sur la question. Ce sont toujours les autorisations d'utilisation d'images qui sont en vigueur (voir Éducaloi) Si on mentionne des RP dans une photo ou un vidéo, la loi 25 s'applique.

Renseignements publics (Gouv Qc, site web, Définitions RP)

Les renseignements qui permettent d'identifier des personnes dans leur entreprise ou leur organisation (nom, titre, fonction, courriel, adresse et no de téléphone du lieu de travail) **sont de nature publique** et ne sont donc pas soumis à la loi 25.

Exemples de renseignement publics

Registre des entreprises
Membre et membres du personnel des organismes publics
Archives judiciaires
Archives municipales
Contractuel avec un organisme public
…

À noter : si on détient des renseignements publics dans nos banques de données pour des raisons autres que les organismes qui les rendent publics, elles deviennent alors des RP soumis à la loi 25.

Par exemple, vous détenez surement des RP du CA de votre organisme pour une utilisation autre que le registraire des entreprises. Ces renseignements sont alors considérés comme des RP.

Renseignements sensibles (Gouv Qc, site web, Définitions RP**)**

> Certains renseignements sont sensibles par leur nature. Il s'agit de renseignement dont on pourrait un usage dommageable pour la personne.

Degré de sensibilité des RP

Faible	Moyen	Élevé
Nom	Adresse postale	Numéro d'assurance sociale
Prénom	No de téléphone	Notes évolutives
Courriel	Date de naissance	Renseignements financiers
		Renseignements médicaux
		Orientation sexuelle
		…

3. Personne responsable de la protection des RP

Obligation (2022) : *Désigner une personne responsable de la protection des renseignements personnels et publier le titre et les coordonnées du responsable sur le site Internet de l'entreprise ou, si elle n'a pas de site, les rendre accessibles par tout autre moyen approprié*.

C'est l'organisation hôte du stockage (qui héberge les données sur son serveur) qui est considérée comme détentrice des données et qui est responsable de l'application de la loi 25.

La personne ayant la **plus haute autorité** dans l'entreprise est **par défaut** responsable de la protection des renseignements personnels. Dans un OCLD il s'agit de la **direction générale**.

Délégation

- Cette fonction peut être déléguée, en tout ou en partie, à une ou plusieurs personnes (par exemple à un comité responsable de la protection des RP)
- On recommande la délégation à une personne qui a un pouvoir décisionnel dans l'organisme.
- La direction générale (responsable par défaut), demeure imputable quant à l'application de la loi 25.
- La direction générale (responsable par défaut), doit appuyer la ou les personnes déléguées en fournissant les ressources humaines, techniques et financières nécessaires.
- Il n'est pas nécessaire d'informer la CAI en cas de délégation.

OUTIL : Formulaire délégation personne responsable

Rôles et fonctions

- Implanter et maintenir la conformité à la loi 25
- En cas d'incident de confidentialité
    - Mettre en place et tenir à jour un registre des incidents
    - Évaluer les risques de préjudice
    - Déclarer les incidents à la CAI et aux personnes concernées
    - Enregistrer les communications à toute personne tierce
    - Assurer le lien avec le fournisseur le cas échéant
- Approuver les politiques et les pratiques de l'entreprise encadrant la protection des RP
- Être le point de contact entre l'organisation et les citoyens
    - Assurer le traitement des différentes demandes des citoyens (accès, rectification, cessation de diffusion, désindexation, réindexation et communication des RP d'une personne décédée)
    - Être disponible pour expliquer à un citoyen les motifs d'un refus, le cas échéant.
- Être le point de contact entre l'organisation et le gouvernement (CAI) dans le cas d'un audit.
- Réaliser une évaluation des facteurs à la vie privée dans le cas
    - D'un projet d'acquisition, de développement ou de refonte d'un système d'information ou de prestation électronique de service ;
    - De la communication de RP à l'extérieur du Québec;
    - De la communication de RP sans consentement dans le cadre d'une recherche, étude ou production de statistiques;
- Mettre en place des mesures préventives
- Offrir de la formation à l'interne
- Se tenir à jour sur son rôle et ses tâches

Publication

Une fois nommée la personne responsable de la protection des RP, les nom, prénom, fonction et responsabilité de la personne en lien avec les RP doivent être communiqués publiquement. La meilleure option est de **publier l'information sur votre site web**.

- Sur votre site web, on peut mettre l'information dans l'onglet « Contact » ou bien créer un onglet « Loi 25 ».

Si vous n'avez pas de site web, vous pouvez :

- Afficher l'information sur votre page Facebook (section « À propos »)
- Créer un message automatisé sur votre téléphone
- (solution minimum) Conserver les informations dans un document à l'interne que vous rendez disponible aux personnes qui fréquentent votre organisme.

4. Incident de confidentialité

Obligations (2022) : *En cas d'incident de confidentialité impliquant un renseignement personnel,*

a. *prendre les **mesures raisonnables** pour **diminuer les risques qu'un préjudice soit causé** aux personnes concernées et **éviter que de nouveaux incidents** de même nature ne se produisent;*
b. aviser la Commission et la personne concernée si l'incident présente un risque de préjudice sérieux;
c. c. tenir un registre des incidents dont une copie devra être transmise à la Commission à sa demande;

Définition

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. Qu'il y ait un risque de préjudice ou non, il s'agit quand même d'un incident de confidentialité.

Exemples d'incident

- Membre du personnel qui consulte un renseignement personnel sans autorisation;
- Membre du personnel qui communique des renseignements personnels au mauvais destinataire;
- L'organisation est victime d'une cyberattaque : hameçonnage, rançongiciel, etc.
- Vol d'ordinateur
- Feu, dégât d'eau

Comment est-ce que je sais que mon organisation a vécu un incident

- Système d'alerte électronique
- Une personne de l'organisation en prend connaissance (ex. vol)
- (Ce qu'on veut éviter) – Une personne extérieure informe l'organisme (ex. envoi courriel frauduleux à tous les contacts)

4.1 Évaluation d'un risque de préjudice

La ou les personnes responsables de la protection des RP doivent faire l'évaluation. Celle-ci peut impliquer d'autres personnes comme le responsable de la sécurité informatique.

Les critères d'évaluation

- La **sensibilité** des renseignements concernés (type RP)
- Les **conséquences** appréhendées de leur utilisation
- La probabilité qu'ils soient utilisés à des **fins préjudiciables / malveillantes**
- La quantité de personnes touchées (plus le nombre est important et plus le risque l'est aussi)
- La reproduction de l'incident (plus l'incident s'est reproduit, plus le risque est important)

Questions à se poser lors de l'évaluation

Qui?	Quelles sont les personnes concernées par l'incident? S'agit-il d'employés, de clients ou de partenaires d'affaires? Qui peut avoir eu accès aux renseignements personnels?
Combien?	Combien de personnes sont touchées par l'incident?
Quoi?	Quelle est la nature des RP visés par l'incident? Sont-ils des renseignements sensibles? Quels sont les risques pour les personnes concernées?
Quand?	Quand l'incident a-t-il eu lieu? Quand a-t-il été découvert?
Où?	Où l'incident a-t-il eu lieu? Au sein de l'organisation? L'incident a-t-il eu lieu chez un tiers détenant des RP pour le compte de l'organisation?
Pourquoi?	Quelles sont les causes? Quelles mesures de sécurité étaient en place au moment de l'incident? Pourquoi n'ont-elles pas été efficaces?

OUTIL : Grille d'analyse du risque de préjudice d'un incident de confidentialité

Actions à prendre selon le résultat de l'évaluation

Risque de préjudice faible	Risque de préjudice moyennement grave ou grave
1. Mettre en place des mesures pour réduire les risques de préjudice et éviter que l'incident se reproduise.	1. Mettre en place des mesures pour réduire les risques de préjudice et éviter que l'incident se reproduise.
2. Inscrire l'incident au registre	2. Inscrire l'incident au registre
	3. Aviser la CAI
	4. Aviser la ou les personnes touchées

4.2 Prendre des mesures pour diminuer les risques

Selon la CAI, les mesures raisonnables à mettre en place **dépendent de l'état de la situation**.

- Toutes les situations sont **différentes**.
- Au besoin, l'organisation continue d'**adapter ses mesures ou à d'en adopter de nouvelles** au fur et à mesure que les circonstances et les impacts de l'incident se précisent par la suite.

Il est fortement conseillé de consulter un service de sécurité informatique pour la mise en place de mesures.

4.3 Les avis à la suite d'un incident

Suite à un incident au risque de préjudice moyennement grave ou grave, la CAI et les personnes touchées doivent être avisées rapidement, soit avec diligence dans les meilleurs délais possible.

Avis à la commission d'accès à l'information

OUTIL : Vous devez remplir et transmettre ce Formulaire d'avis à la CAI.

- Suite à l'envoi, toute nouvelle information doit également être transmise.
- Suite au traitement de l'avis, la CAI peut exiger à votre organisme l'application de toutes mesures visant à protéger les droits, la remise des renseignements personnels ou leur destruction et ordonner d'informer la personne concernée si ce n'est pas déjà fait.

Avis à la personne concernée

- Les personnes doivent être avisées personnellement par courriel, par envoi postal, par téléphone ou en personne.
- Si on est incapable de joindre la personne, on doit publier un avis public d'incident sur notre site internet.

Ce que l'avis à la personne concernée doit contenir

- Une **description des renseignements personnels visés par l'incident** (type RP). Si cette information n'est pas connue, l'organisation doit communiquer la raison justifiant l'impossibilité de fournir cette description.
- Une brève description des **circonstances** de l'incident.
- La **date ou la période où l'incident** a eu lieu, ou une approximation de cette période si elle n'est pas connue.
- Une brève description des **mesures prises ou envisagées pour diminuer les risques** qu'un préjudice soit causé à la suite de l'incident.
- Les **mesures proposées à la personne concernée** afin de diminuer le risque qu'un préjudice lui soit causé ou d'atténuer celui-ci.
- Les **coordonnées d'une personne ou d'un service** avec qui la personne concernée peut communiquer pour obtenir davantage d'informations au sujet de l'incident.

OUTILS : Modèle lettre avis incident gouv. QC.

Avis à une personne tierce

L'organisation peut aviser toute personne ou organisme susceptibles de diminuer le risque de préjudice sérieux. Seuls les renseignements personnels nécessaires peuvent alors être communiqués, sans le consentement de la personne concernée. Le responsable de la protection des renseignements personnels de l'organisation doit enregistrer cette communication.

4.4 Registre des incidents

Le registre inclut les incidents avec et sans risque de préjudice.

Le registre doit inclure

- Une **description des renseignements personnels** visés par l'incident. Si cette information n'est pas connue, l'organisation doit inscrire la raison justifiant l'impossibilité de fournir cette description.
- Une brève description des **circonstances** de l'incident;
- La **date ou la période où l'incident a eu lieu**, ou une approximation de cette période si elle n'est pas connue;
- La **date ou la période au cours** de laquelle l'organisation a **pris connaissance** de l'incident;
- Le **nombre de personnes concernées** par l'incident ou, s'il n'est pas connu, une approximation de ce nombre;
- Une description des éléments qui amènent l'organisation à conclure **qu'il y a, ou non, risque qu'un préjudice sérieux** soit causé aux personnes concernées (*voir évaluation*)
- Les **dates de transmission des avis à la Commission et aux personnes concernées**, quand l'incident présente le risque de préjudice sérieux. L'organisation doit aussi préciser si elle a donné des avis publics et la raison de ceux-ci;
- Une brève description des **mesures prises par l'organisation** à la suite de l'incident, pour diminuer les risques qu'un préjudice soit causé.

Lors d'un incident, il est important de tenir une liste des personnes concernées. C'est une information qui est demandée lors d'un audit informatique. Les informations sur cette liste sont considérées comme des RP soumis à la loi 25.

Les renseignements du registre doivent être mis à jour et conservés pour une **période minimale de cinq ans**, après la date ou période de prise de connaissance de l'incident par l'organisation.

OUTIL : Modèle registre des incidents de confidentialité

BLOC 2

Le cycle de vie des renseignements personnels

Le cycle de vie des RP se décline en cinq grandes étapes :

- La collecte
- L'utilisation
- La communication
- La conservation
- La destruction

1. Collecte des RP

Obligations :

- **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;

Évaluation de la nécessité d'un RP

1. L'objectif poursuivi doit être légitime, important et réel ;
2. La collecte de RP doit être rationnellement liée et nécessaire à l'atteinte de l'objectif ;
3. L'atteinte à la vie privée à la suite de la collecte, de la communication et de la conservation doit être proportionnelle à l'objectif visé.
    - La collecte peut être faite si elle est nettement plus utile à l'organisme ou à l'entreprise que préjudiciable à la personne concernée.
    - L'atteinte à la vie privée doit être minimisée.

2. Utilisation des RP

L'utilisation est la période pendant laquelle le RP est utilisé par les personnes autorisées au sein de l'entreprise.

Obligations (2023) : *Respecter les nouvelles règles d'utilisation des renseignements personnels.*

- **Limiter l'accès aux renseignements personnels** aux seules personnes ayant la qualité pour les recevoir au sein de l'entreprise lorsque ces renseignements sont nécessaires à l'exercice de leurs fonctions ;
- **Limiter l'utilisation des renseignements personnels** : à moins d'une exception prévue par la loi, l'entreprise doit obtenir le consentement de la personne concernée pour utiliser ses renseignements une fois l'objet du dossier accompli.

3. Communication des RP

La communication est la période où le renseignement personnel est communiqué, par exemple dans un système de prestation électronique de services, par courriel, au service à la clientèle, par le biais de sites web ou à un tiers.

Obligation (2022) : *Respecter le nouvel encadrement de la communication de renseignements personnels sans le consentement de la personne concernée à des fins d'étude, de recherche ou de productions de statistiques et dans le cadre d'une transaction commerciale;*

(2023) *Respecter les nouvelles règles de communication de renseignements personnels sans le consentement de la personne concernée (exercice d'un mandat ou exécution d'un contrat de service ou d'entreprise);*

(2023) *Respecter les nouvelles règles de communication des renseignements personnels à l'extérieur du Québec;*

Communication et consentement

Il est nécessaire d'obtenir le consentement de la personne concernée si vous communiquez ses RP. Bien qu'il existe des exceptions à cette règle, l'obtention du consentement devrait être privilégiée.

Diffusion de RP sur internet

Si vous diffusez des RP sur le web (votre site web, page Facebook…), assurez-vous d'avoir les moyens de faire disparaître ces informations ultérieurement.

CAS D'EXCEPTION – Communication à l'extérieur du Québec

Si vous devez communiquer les RP d'une personne à l'extérieur du Québec (par exemple à un fournisseur), vous devez :

1. Informer la personne concernée
2. Réaliser une évaluation des facteurs à la vie privée (ÉFVP)
3. S'assurer de mesures de protection adéquate lors du transfert
4. Faire signer une entente écrite avec le tiers

EXCEPTIONS – Communication des RP sans consentement

Il est nécessaire de bien s'informer auprès de la CAI ou d'un avocat spécialisé si vous souhaitez communiquer des RP sans le consentement de la personne concernée. Certains cas de figure s'accompagnent d'obligations particulières.

Quelques exemples d'exceptions

- En cas d'urgence ou en vue de prévenir un acte de violence.
- Communication à des fins judiciaires ou d'enquête
- Dans le contexte d'une étude, recherche ou production statistique (besoin de réaliser une évaluation des facteurs à la vie privée)
- Dans le cas d'un incident de confidentialité
- …

4. Conservation des RP

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

Obligations :

- **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**.

Mise en place d'une procédure de gestion documentaire

La CAI recommande de mettre en place une procédure de gestion documentaire qui

- Inventorie les types de documents contenant des RP
- Définie les niveaux de confidentialité des documents (protégé, confidentiel et secret) en fonction de
  - la sensibilité
  - la finalité
  - la quantité
  - la répartition et
  - le support.
- Distingue les types de supports et y associe une méthode de conservation (emplacement) et de destruction appropriée
- Détermine un calendrier de conservation respectant les exigences légales

OUTIL : Inventaire des RP

5. Destruction des RP

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

Obligations (2023) : *Détruire les renseignements personnels lorsque la finalité de leur collecte est accomplie, ou les anonymiser pour les utiliser à des fins sérieuses et légitimes, sous réserve des conditions et d'un délai de conservation prévus par une loi;*

Procédure de destruction

La méthode de destruction doit être adaptée au support et au niveau de confidentialité des documents et assurer la destruction définitive des renseignements personnels qu'ils contiennent.

Vous pouvez détruire vous-même les documents contenant des renseignements personnels. Si votre équipement ne vous permet pas de le faire de manière sécuritaire, vous pouvez aussi conclure un contrat avec un prestataire externe. Par exemple, la destruction définitive des données contenues dans un disque dur peut nécessiter le recours à une firme externe.

Support	Exemples de méthodes de destruction
Papier (original et toutes les copies)	Déchiqueteuse, de préférence à découpe transversale. Si les documents sont très confidentiels : déchiqueteuse + incinération
Média numérique que l'on souhaite réutiliser ou recycler Ex. Carte de mémoire flash (carte SD, XD, etc.), clé USB, disque dur d'ordinateur	Formatage, réécriture, déchiquetage numérique (logiciel effectuant une suppression sécuritaire et qui écrira de l'information aléatoire à l'endroit où se trouvait le fichier supprimé).
Média numérique non réutilisable Ex. Certains CD, DVD, carte de mémoire flash, clé USB et disque dur qui ne seront plus utilisés	Destruction physique (déchiquetage, broyage, meulage de surface, désintégration, trouage, incinération, etc.). La plupart des déchiqueteuses pourront détruire les CD et les DVD.
Machines contenant des disques durs Ex. Photocopieur, télécopieur, numériseur, imprimante, etc.	Démagnétiseur pour les disques durs. Écrasement des informations sur le disque dur ou disque dur enlevé et détruit lorsque les machines sont remplacées.

Anonymisation des RP

Un renseignement anonymisé est un renseignement qui ne permet plus, de façon irréversible, d'identifier directement ou indirectement la personne concernée.

À la lumière des avancées technologiques actuelles et futures, la CAI estime qu'il est **quasi impossible de certifier que des renseignements anonymisés ne pourraient pas éventuellement être réidentifiés**.

Nous vous conseillons donc fortement de simplement détruire les RP que votre organisme détient selon les délais prescrits.

6. Fournisseurs

Dans divers contextes, les organisations confient des renseignements personnels à des tiers qui en assurent la conservation. Les organisations demeurent malgré tout responsables de l'ensemble des leurs obligations en cas d'incident de confidentialité :

- mesures à prendre,
- registre à tenir et à mettre à jour,
- avis à donner,
- etc.

Le fournisseur est dans l'obligation d'aviser sans délai le responsable de la protection des RP dans le cas d'un incident de confidentialité.

Les différents types de fournisseurs et les obligations en matière de protection des RP

Type de fournisseur	Obligations
1. **Qui a accès aux RP** Ex. technicien informatique, comptable, etc.	Avoir une entente signée assurant le respect de la confidentialité des données
2. **Qui loue un espace pour déposer les RP** Ex. Microsoft 365, Suite Google, etc.	Votre organisme demeure responsable de sécuriser cet espace.
3. **Qui détient des RP de l'organisme** (aucun contrôle par le bénéficiaire) Ex. Plateforme de gestion des RH, comptable, sauvegarde, etc.	Vous êtes responsable de vous assurer d'avoir une entente écrite avec le fournisseur qui détaille : • Ce qu'il fait avec les RP • Les mesures de sécurité mises en place tout au long du cycle de vie des RP (sauvegardes, destruction, etc.) • L'obligation de déclaration en cas d'incident de confidentialité
4. Qui détient les RP de l'organisme et se trouve **à l'extérieur du Québec**	Besoin d'une clause supplémentaire au contrat qui indique comment sont protégés les RP lors du transfert des données

Valider sa conformité à la loi 25 avec ses fournisseurs

1. Lister vos fournisseurs.
2. Identifier pour chacun de quel type de fournisseur il s'agit.

S'il s'agit d'un fournisseur qui détient vos RP

3. Inscrire à l'inventaire des RP dans l'onglet fournisseur

S'il s'agit d'un fournisseur qui détient vos RP

4. Vérifier les politiques d'utilisation de l'entreprise. Si vous trouvez les informations nécessaires dans la politique, inscrire l'emplacement dans l'inventaire.
5. Si vous ne trouvez pas les informations nécessaires, appeler le fournisseur et vérifier s'ils ont une politique en vertu de la loi 25.
6. S'ils n'ont pas de politique, vous êtes responsable de leur fournir un contrat à signer.
7. S'ils ne veulent pas signer le contrat, envisager de trouver un autre fournisseur.

OUTILS

- Formulaire d'engagement de confidentialité

BLOC 3

1. Politique de confidentialité et de protection des renseignements personnels

Obligation (2023) : *Avoir établi des politiques et des pratiques encadrant la gouvernance des renseignements personnels et publier de l'information détaillée sur celles-ci en termes simples et clairs sur le site Internet de l'entreprise ou, si elle n'a pas de site, par tout autre moyen approprié*

Une politique adaptée

- Il n'existe pas de politique qui fonctionne pour l'ensemble des organisations. La politique doit :
  - refléter les pratiques de votre organisme ;
  - être évolutive en fonction de ces pratiques et ;
  - être proportionnelle à l'importance des activités de l'organisme.

Ce que doit contenir la politique

- Le détail de la gouvernance des RP tout au long de leur cycle de vie
  - Collecte
    - Comment sont recueillis les RP?
    - Quels types de RP sont recueillis?
    - Y a-t-il consentement a la collecte?
  - Utilisation
    - Pourquoi ces RP sont-ils collectés?
    - Qui a accès aux RP?
  - Conservation
    - Où sont conservés les RP?
    - Sauvegarde? Archive?
  - Communication
    - À qui ces RP sont-ils communiqués?
  - Destruction
    - Quel est le processus de destruction des RP?
    - Quels sont les délais de conservation des RP?
- Les contrôles et mesures de sécurité mises en place
- Les rôles et responsabilités des membres du personnel
- Un processus de traitement des plaintes relatives à la protection des RP

La politique peut également inclure

- Le public cible (à qui s'adresse la politique?)
- Les dates de création et de révision
- Le contexte de la politique
- Les définitions utilisées

La diffusion de votre politique

Une fois rédigée votre politique, vous devez la publier **sur votre site web**.

Si vous n'avez pas de site web, vous pouvez :

- Afficher l'information sur votre page Facebook (section « À propos »)
- Créer un message automatisé sur votre téléphone
- (solution minimum) Conserver les informations dans un document à l'interne que vous rendez disponible aux personnes qui fréquentent votre organisme.

Entente de confidentialité avec les employé.e.s

- Vous devez avoir des ententes de confidentialité signées avec vos employé.e.s assurant leur respect de la politique de confidentialité de l'organisme.
- Cette entente peut prendre la forme d'une clause au contrat de travail.
- L'entente peut inclure :
    - L'engagement à respecter la politique en matière de protection des RP de l'organisme ;
    - L'engagement à utiliser des données confidentielles seulement dans l'exercice des obligations de travail ;
    - L'engagement à ne pas divulguer à quiconque les RP ou permettre qu'ils ne soient divulgués, sauf pour la réalisation des activités ;
    - L'engagement qui lie l'employé au-delà de la fin du contrat de travail en matière de confidentialité.

OUTILS

- Modèle de politique de confidentialité
- Formulaire d'engagement de confidentialité

2. Le consentement

Obligations (2023)

Respecter les nouvelles règles entourant le consentement à la collecte, à la communication ou à l'utilisation des renseignements personnels ;

Respecter vos nouvelles obligations d'information et de transparence envers les citoyens ;

Respecter le droit à la cessation de la diffusion, à la réindexation ou à la désindexation (ou droit à l'oubli) ;

Respecter les nouvelles règles entourant la collecte de renseignements personnels concernant un mineur ;

Cas d'exception – Collecte de RP auprès d'un tiers

La loi 25 prévoit certaines situations où l'on peut recueillir des RP auprès d'un tiers sans le consentement de la personne concernée. Si vous vous retrouvez dans une telle situation, il est important de bien s'informer auprès de la CAI de vos responsabilités et obligations.

2.1 Droit à l'information et transparence

Au-delà des protections légales, la sensibilisation et la responsabilisation du citoyen à l'importance de la protection de ses renseignements personnels sont nécessaires. Avant de consentir à la collecte d'un renseignement personnel, la personne concernée doit pouvoir comprendre pourquoi l'entreprise ou l'organisme recueille ses renseignements personnels.

Informations à fournir avant la collecte de RP (et qui doivent se trouver dans votre avis de consentement)

- **Qui?** L'organisation qui collecte et/ou communique les RP
  - ~~Le cas échéant, le nom du tiers pour qui la collecte est faite~~
- **Pourquoi?** Objectifs pour lesquels les RP sont recueillis
- **Quoi?** RP ou catégories de RP recueillies
- **Comment?** Moyens par lesquels les RP sont recueillis
- **Communication?** (le cas échéant)
  - Le nom du tiers ou des **catégories de tiers** à qui les RP seront **communiqués**
  - La possibilité que les RP soient **communiqués à l'extérieur du Québec**
- **Droit de retirer son consentement** à la communication ou à l'utilisation des RP recueillis
  - La personne peut refuser de donner son consentement au moment de la collecte ou peut le retirer ultérieurement.
- Droits d'accès et de rectification prévus par la Loi
- **Accès?** Personnes ou catégorie de personnes dans l'organisation qui auront accès aux RP
- **Durée** de validité du consentement
  - Délai *x* ou à la suite d'un événement *y*
- Nom et coordonnées de la **personne responsable** de la protection des RP

Présentation de l'information

Il est important de ne pas surcharger le formulaire de consentement. L'information peut être présentée en plusieurs niveaux. Par exemple :

1. **Premier niveau**
    a. Objectif de la collecte
    b. RP concernées
    c. Le cas échéant, le tiers à qui l'on communique les RP
2. **Second niveau.** On y retrouve le reste des informations. Il pourrait s'agir de :
    a. Votre politique de confidentialité
    b. Une annexe au formulaire
    c. …

2.2 Critères de validité du consentement

Pour être valide, le consentement d'une personne doit être :

- **Manifeste**: évident et donné d'une façon qui démontre la volonté réelle de la personne concernée ;
- **Libre**: impliquant un réel choix et donné sans contraintes ou pression indue ;
- **Éclairé** : précis, donné en toute connaissance de cause et avec toutes les informations nécessaires pour comprendre la portée du consentement ;
- **Spécifique**: donné dans un objectif précis et clairement circonscrit ;
- **Temporaire** : valide seulement pour la durée nécessaire à la réalisation des fins auxquelles il a été demandé ;
    - Si votre organisation demande le consentement **pour une longue durée**, il est conseillé de faire un rappel du consentement ponctuellement à la personne concernée ;
- **Granulaire**: demandé pour chaque fin spécifique ;
- **Compréhensible** : demandé en des termes simples et clairs ;
- **Distinct** : demandé distinctement de toute autre information, lorsque la demande est faite par écrit ;
    - L'avis de consentement peut être envoyé à l'intérieur d'une autre communication, par exemple une infolettre, mais il doit constituer une section distincte et clairement identifiée.

2.3 Les consentements implicite et explicite

Implicite	Explicite
Pour les RP non sensibles	Pour les RP sensibles
Formule *opt out* :	Formule *opt in* :
Libellé de consentement qui inclut une procédure pour que la personne puisse vous informer en cas de refus (contact personne responsable des RP)	Libellé de consentement avec signature, bouton cliquable en ligne… Le consentement doit être exprimé de façon expresse : par un geste ou une déclaration (orale ou écrite) témoignant de l'acceptation. Il ne laisse alors aucun doute sur la volonté réelle de la personne.
Si on n'a pas de retour, la personne est réputée consentir	Si on n'a pas de retour, la personne est réputée ne pas consentir

2.4 Les moyens d'obtenir le consentement

Vous pouvez obtenir le consentement d'une personne :

- À l'oral en personne (consigner dans un registre) ;
- Par échange courriel ;
- Par téléphone ;
- Par un formulaire de consentement signé.

La meilleure option demeure toujours le formulaire de consentement signé. Dans le cas de la collecte de RP sensibles, on devrait privilégier le formulaire signé ou l'enregistrement audio d'une conversation téléphonique.

2.5 Consentement et finalités multiples

Un formulaire de consentement peut concerner **plusieurs finalités différentes**, toutefois :

- La personne doit pouvoir donner ou refuser son consentement **pour chacune des finalités différentes** ;
- Un consentement implicite devrait donc généralement n'impliquer qu'une seule finalité.
- Les informations relatives aux finalités primaires et aux finalités secondaires de la collecte doivent être présentées de manière distincte (sections différentes) ;

2.6 Le consentement pour les personnes mineures

Moins de 14 ans

- Le consentement peut uniquement être donné par le parent ou le tuteur
  - RP non sensibles = consentement implicite
  - RP sensibles = consentement explicite
- Exceptions
  - Si le parent ou le tuteur a préalablement donné son autorisation
  - S'il s'agit d'une situation « manifestement au bénéfice de la personne mineure » (situation médicale d'urgence, dossier de protection de la jeunesse, etc.)

14 ans ou plus

- Le consentement peut être donné par le jeune ou le parent ou tuteur
  - RP non sensibles = consentement implicite
  - RP sensibles = consentement explicite
- Un organisme public devrait considérer notamment la sensibilité des renseignements, la complexité de la demande ainsi que les enjeux et les répercussions pour déterminer s'il est préférable d'obtenir le consentement à la fois de la personne mineure de 14 ans ou plus et du ou de la titulaire de l'autorité parentale ou encore de la tutrice ou du tuteur.

Personne mineure simplement ou pleinement émancipée

- Le consentement peut uniquement être donné par le jeune.

2.7 Consentement des personnes dont on détient déjà les RP

Vous devez transmettre un avis de consentement à tous les individus dont votre organisme détient des RP. Si vous n'obtenez pas le consentement, ces RP devront être détruits.

On recommande de retransmettre ponctuellement l'avis de consentement pour le renouveler.

2.8 Refus de consentement et participation aux activités

Sous réserve de quelques exceptions prévues par la loi, une entreprise ne peut refuser d'accorder un bien ou un service ni rejeter une demande relative à un emploi parce que la personne qui formule la demande refuse de lui fournir un renseignement personnel.

Par contre, il arrive que l'utilisation et/ou la communication des RP soient **nécessaires** à la réalisation d'un service ou d'une embauche et **liées à la finalité primaire de l'organisation**. Dans ce cas, l'organisation se trouve dans son droit de refuser de fournir un service ou d'embaucher quelqu'un. **L'organisation doit alors s'assurer de la nécessité des RP.**

Les organisations doivent toutefois permettre aux personnes le refus de consentement pour toutes collecte, utilisation et/ou communication qui répond à une finalité secondaire de l'organisation.

Avant même d'aller obtenir les consentements nécessaires, on recommande de **déterminer à l'avance quels services ne pourront pas être offerts en cas de refus de consentement.**

OUTIL : Modèle de formulaires de consentement

3. Demandes des citoyens

Obligations (2023)

Respecter le droit à la cessation de la diffusion, à la réindexation ou à la désindexation (ou droit à l'oubli);

Respecter les nouvelles règles de communication des renseignements personnels facilitant le processus de deuil.

(2024) *Répondre aux demandes de portabilité des renseignements personnels.*

Toutes les demandes des citoyens doivent être formulées à l'écrit (par courrier ou courriel)

3.1 Réponse à la demande

Le responsable de la protection des RP doit répondre à la demande par écrit dans les 30 jours suivants sa réception. L'absence de réponse dans ce délai équivaut à un refus.

À la réception d'une demande d'un citoyen, expliquez la procédure au citoyen :

1. Remplir le formulaire de la CAI
2. Le transmettre à la personne responsable de la protection des RP
3. Délai de réception de la réponse (30 jours)

Vous pouvez également référer le citoyen à cette page de la CAI → questions fréquentes

Dans le cas d'un refus

- Assurez-vous auprès de la CAI ou d'un avocat spécialisé des motifs valables de refus et de la démarche à suivre
- Vous devez inscrire toutes les raisons valables dans l'avis de refus.

3.2 Demande d'accès

Informations à fournir sur demande :

- Renseignements personnels qui sont recueillis auprès de la personne ;
- Catégories de personnes qui ont accès à ces renseignements au sein de l'entreprise ;
- Durée de conservation des renseignements personnels ;
- Coordonnées du responsable de la protection des renseignements personnels.

3.3 Droit à la rectification

Le droit à la rectification est le droit de faire modifier tout renseignement personnel inexact, incomplet ou équivoque dans une base de données.

3.4 Droit à l'oubli

Le droit à l'oubli est le droit de demander la suppression de ses RP d'une base de données. C'est quelque chose de complexe avec beaucoup de spécificités. Si vous vous retrouvez dans cette situation, informez-vous auprès de la CAI ou d'un avocat spécialisé.

3.5 Droit à la cessation de diffusion, à la réindexation ou à la désindexation

Une personne peut demander :

- La cessation de la diffusion de ses renseignements personnels ;
- La désindexation d'un hyperlien rattaché à leur nom et donnant accès à leurs renseignements par un moyen technologique.

Les personnes concernées pourront faire ces demandes dans l'un des cas suivants :

- Si la diffusion de leurs renseignements contrevient à la Loi ou à une ordonnance judiciaire;
- Si la diffusion de leurs renseignements personnels leur cause un préjudice grave lié au droit du respect de leur réputation ou de leur vie privée. Dans ce cas, ils pourront aussi en demander la réindexation. La Loi prévoit certaines conditions.

Si cette demande est acceptée, l'avis devra attester de la cessation de diffusion des renseignements, de la désindexation ou de la réindexation de l'hyperlien.

3.6 Droit à la portabilité

Le droit à la portabilité est simplement le droit de recevoir ses renseignements personnels informatisés dans un format technologique structuré, simple et couramment utilisé (ex. pdf, word, xlsx…).

3.7 Communication des RP d'une personne décédée

Les renseignements personnels d'une personne décédée pourront être communiqués à son conjoint ou à l'un de ses proches parents si le fait de connaître ce renseignement est susceptible d'aider cette personne dans son processus de deuil. Une restriction s'appliquera, cependant, si une personne décédée a préalablement consigné, par écrit, son refus d'accorder ce droit d'accès.

Si vous vous retrouvez dans une telle situation, vous pouvez trouver davantage d'information sur ces pages web du gouvernement du Québec :

→ Deuil
→ Succession

OUTIILS : Formulaires CAI demandes citoyens (voir « Formulaires dans les entreprises privées »)

BLOC 4

1. Évaluation des facteurs relatifs à la vie privée (ÉFVP)

Obligations

(2022) *Procéder à une évaluation des facteurs relatifs à la vie privée (ÉFVP) avant de communiquer des renseignements personnels sans le consentement des personnes concernées à des fins d'étude, de recherche ou de production de statistiques ;*

(2023) *Réaliser une évaluation des facteurs relatifs à la vie privée (ÉFVP) lorsque la Loi l'exige, par exemple avant de communiquer des renseignements personnels à l'extérieur du Québec.*

L'ÉFVP est une démarche d'analyse visant à protéger les RP et protéger la vie privée. Un guide d'accompagnement à suivre lors de sa réalisation est diffusé par la CAI. Elle doit être réalisée dans certaines situations spécifiques.

Moments où l'on doit réaliser une ÉFVP

- Projets d'acquisition, de développement et de refonte d'un système d'information ou de prestation électronique de services impliquant des renseignements personnels ;
- Communication de RP à l'extérieur du Québec ;
- Communication de RP sans consentement dans le cadre d'une recherche, étude ou production de statistiques.

OUTIL : Guide d'accompagnement évaluation des facteurs à la vie privée

2. Sécurité informatique (pistes)

Obligations (2023) : *Prévoir, par défaut, les paramètres assurant le plus haut niveau de confidentialité du produit ou du service technologique offert au public.*

Certaines entreprises comme GCV informatique offrent un accompagnement dans la mise en conformité à la Loi 25 et dans la mise à jour des mesures de sécurité de votre parc informatique.

Antivirus

- Un bon antivirus peut générer des alertes au niveau informatique pour savoir si votre organisation est touchée par un incident de confidentialité.

Stockage infonuagique

- Les espaces de stockage infonuagique comme Microsoft 365 ou Google Suite ne sont pas protégés d'emblée.
- Il faut voir avec un service informatique pour protéger ces espaces.

Courriel

- Les boîtes courriel doivent être protégées avec un système qui permet de valider et d'analyser ce qui est envoyé et reçu.
  - Ça permet d'avoir beaucoup d'informations et de moyens en cas de fraude (courriel frauduleux, rançongiciel…)
- Les adresses courriel avec des noms de domaine public comme @hotmail.com, @outlook.com, @yahoo.com, @gmail.com… ne peuvent pas être protégées. Il est déconseillé fortement de les utiliser à des fins professionnelles.
- Options de protection des courriels
  - Cryptage des courriels
  - Partage d'informations sensibles par organisation tierce (ex. Bitwarden)

Mots de passe ordinateurs et biométrie

- Programmer de bons mots de passe sur les ordinateurs
  - 12 caractères minimums avec majuscule, minuscule et caractères spéciaux
- La biométrie (empreintes digitales ou reconnaissance faciale) peut aussi être utilisée pour verrouiller les ordinateurs
  - C'est aussi efficace qu'un bon mot de passe
  - La loi 25 contient plusieurs obligations particulières relatives à la biométrie
- À noter : si les ordinateurs ne sont pas protégés pour qu'on ne puisse pas en retirer les informations (cryptage des disques durs), un fraudeur va pouvoir accéder aux données, peu importe les mots de passe ou l'utilisation de la biométrie.

Sauvegarde des données

- Dans le cas d'un rançongiciel, il est important de prévoir avoir une sauvegarde des données.

OUTIL : Bonnes pratiques en matière de protection des RP (gouv. Qc.)

Récapitulatif – À faire et outils

Bloc 1

À FAIRE

1. Vérifier auprès de mes assurances que je suis protégé en cas de litige
2. Nommer une personne responsable des RP
3. Publier l'information sur mon site internet
4. M'approprier le registre des incidents
5. Solliciter les membres de mon équipe afin qu'ils :
   a. listent l'ensemble des RP qu'ils détiennent et
   b. se rendent disponible pour rencontrer le responsable des RP au moment de faire l'inventaire.

OUTILS

1. Formulaire délégation CAI
2. Grille d'analyse du risque de préjudice d'un incident de confidentialité
3. Formulaire d'avis à la CAI
4. Modèle lettre avis incident gouv. Qc
5. Procédure en cas d'un incident de confidentialité
6. Registre des incidents de confidentialité

Bloc 2

À FAIRE

1. Réaliser l'inventaire des RP
2. Valider que vous avez une entente de protection adéquate auprès de vos fournisseurs

OUTILS

1. Inventaire des RP

Bloc 3

À FAIRE

1. Rédiger une politique de confidentialité et la publier sur son site internet
2. Faire signer des ententes de confidentialité avec les employé.e.s de l'organisme
3. Rédiger un formulaire de consentement
4. Transmettre un avis de consentement aux personnes dont on a déjà les RP
5. Déterminer quels services ne pourront pas être offerts en cas de refus de consentement

OUTILS

1. Modèle de politique de confidentialité
2. Formulaire d'engagement de confidentialité
3. Modèle de formulaires de consentement
4. Formulaires CAI demandes citoyens

Bloc 4

À FAIRE

1. Mettre en place les mesures de sécurité et cybersécurité nécessaires à la protection des RP.

OUTILS

1. Guide d'accompagnement évaluation des facteurs à la vie privée
2. Bonnes pratiques en matière de protection des RP (gouv. Qc.)

RÉFÉRENCES

Commission d'accès à l'information, site web, Aide-mémoire : résumé des nouvelles obligations des entreprises

GCV Informatique, Loi 25 : Trousse de conformité administrative

TRPOCB, site web, Nouvelles dispositions protégeant la vie privée des Québécois

BLOC 1 : Définitions de concepts, personne responsable de la protection des RP et incidents de confidentialité

Commission d'accès à l'information, site web, Cadre général d'application des sanctions

Commission d'accès à l'information, site web, Communiquer des RP sans le consentement de la personne concernée

Commission d'accès à l'information, site web, Responsable de la protection des RP

Commission d'accès à l'information, site web, Incident de confidentialité impliquant des RP

Commission d'accès à l'information, site web, Prendre des mesures pour diminuer les risques

Commission d'accès à l'information, site web, Évaluer les risques

Commission d'accès à l'information, site web, Aviser la commission et les personnes concernées

Commission d'accès à l'information, site web, Registre des incidents de confidentialité

Éducaloi, site web, Le droit à l'image

Gouvernement du Québec, site web, Définition de mots en lien avec la protection des RP

BLOC 2 : Cycle de vie des données et inventaire des RP

Commission d'accès à l'information, site web, Protection des renseignements personnels

Commission d'accès à l'information, site web, La collecte des renseignements

Commission d'accès à l'information, site web, Consentement en matière de RP

Commission d'accès à l'information, site web, Informations à fournir avant la collecte de RP

Commission d'accès à l'information, site web, Communiquer des RP sans le consentement de la personne concernée

Commission d'accès à l'information, site web, Communication de RP à l'extérieur du Québec

Commission d'accès à l'information, site web, Communication de RP sans consentement à des fins de recherche

Commission d'accès à l'information, site web, Communication de RP en cas d'urgence en vue de prévenir un acte de violence

Commission d'accès à l'information, site web, Procédure de destruction

Commission d'accès à l'information, site web, Responsable de la protection des RP

Commission d'accès à l'information, site web, Destruction et anonymisation

Gouvernement du Québec, site web, Anonymisation

BLOC 3 : Politique de confidentialité, consentement et demandes des citoyens

Commission d'accès à l'information, site web, Protection des renseignements personnels

Commission d'accès à l'information, site web, Politique confidentialité

Commission d'accès à l'information, site web, Informations à fournir avant la collecte de RP

Commission d'accès à l'information, site web, La collecte des renseignements

Commission d'accès à l'information, site web, Consentement en matière de RP

Commission d'accès à l'information, site web, Les dossiers personnels dans les entreprises privées

Commission d'accès à l'information, site web, Responsable de la protection des RP

Gouvernement du Québec, site web, Nouveautés liées au consentement

Gouvernement du Québec, site web, Personne autorisée à donner son consentement

Gouvernement du Québec, site web, Droit à la portabilité

Gouvernement du Québec, site web, Accès aux RP lors d'un processus de deuil

Gouvernement du Québec, site web, Accès aux RP lors d'une succession ou lors d'une prestation de décès

BLOC 4 : Évaluation des facteurs relatifs à la vie privée (ÉFVP) et sécurité informatique (pistes)

Commission d'accès à l'information, site web, Biométrie

Commission d'accès à l'information, site web, L'évaluation des facteurs relatifs à la vie privée