



La loi 25...

Le guide d'application, étape par étape

C'est le 22 septembre 2022 qu'entraient en vigueur certaines dispositions de la loi 25. Cette réforme vise à moderniser les règles protégeant les renseignements personnels au Québec afin qu'elles soient mieux adaptées aux nouveaux défis posés par l'environnement numérique et technologique. Rappelons que les modifications apportées par la Loi 25 entrent progressivement en vigueur sur une période de trois ans, jusqu'en 2024.

Qu'est-ce qu'un renseignement personnel ?

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.

Les renseignements d'identification :

L'adresse, le numéro de téléphone, le sexe, l'âge, le numéro d'assurance sociale, le numéro d'assurance maladie, l'identifiant numérique, etc.

Renseignements de santé :

Le dossier médical, un diagnostic, une consultation d'une professionnelle ou d'un professionnel de la santé, les médicaments, les ordonnance, les renseignements sur la cause d'un décès, etc.

Renseignements financiers :

Le revenu d'une personne, les renseignements relatifs à l'impôt, le numéro de compte bancaire, les biens possédés, les numéros de cartes de crédit, etc.

Renseignements relatifs au travail :

Le dossier disciplinaire, les motifs d'absence, les dates de vacances, le salaire, l'évaluation du rendement, les heures d'entrée et de sortie liées au lieu de travail, etc.

Renseignements scolaires et relatifs à la formation :

L'inscription à des cours, le choix de cours, les résultats scolaires, les diplômes, le curriculum vitae, etc.

Renseignements relatifs à la situation sociale ou familiale :

Les documents qui attestent l'état civil, le fait qu'une personne ait ou non des enfants ou qu'elle reçoive des prestations d'aide sociale ou de chômage, etc.

Depuis 22 septembre 2022



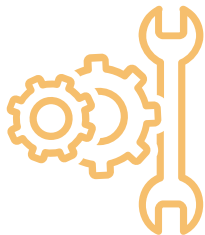
Si vous êtes la plus haute autorité de l'entreprise et que vous ne souhaitez pas exercer la fonction de **responsable de la protection des renseignements personnels**, désignez une personne pouvant assumer efficacement ce rôle. Par exemple, celle-ci devrait avoir les compétences requises et un pouvoir décisionnel important;



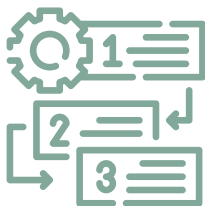
Appuyez la personne responsable de la protection des renseignements personnels avec les **ressources nécessaires** (humaines, techniques et financières) pour assurer la réussite de votre mise en conformité;



Faites **l'inventaire des renseignements personnels** détenus par votre entreprise (ou pour son compte par un tiers) et évaluez leur sensibilité; (voir l'[annexe 1](#))



Mettez en place des **mesures pour prévenir ou limiter les conséquences d'un incident** de confidentialité impliquant un renseignement personnel; (voir l'[annexe 2](#))



Instaurez des pratiques qui vous permettront de **réagir adéquatement et rapidement** en cas d'incident de confidentialité impliquant un renseignement personnel (ex. : plan de réponse aux incidents et directive au personnel); (voir l'[annexe 3](#))



Si vous prévoyez utiliser une technique biométrique (ex. : empreinte digitale, reconnaissance faciale ou vocale), **informez-vous au préalable de vos obligations** en la matière. (voir l'[annexe 4](#))

OBLIGATIONS		EN PROCESSUS	FAIT
1	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.	☐	☐
2	En cas d'incident de confidentialité impliquant un renseignement personnel		
	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.	☐	☐
	<u>Aviser la Commission et la personne concernée</u> si l'incident présente un risque de préjudice sérieux (<u>vidéo expliquant ce qu'est un risque réel de préjudice grave</u>).	☐	☐
	Tenir un registre des incidents dont une copie devra être transmise à la Commission à sa demande.	☐	☐
3	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.	☐	☐
4	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	☐	☐
5	Divulguer préalablement à la Commission la vérification ou la confirmation d'identité faite au moyen de caractéristiques ou de <u>mesures biométriques</u> .	☐	☐

Depuis 22 septembre 2023

Pour établir et mettre en œuvre vos **politiques de gouvernance en matière de protection des renseignements personnels**, veuillez vous référer au [Guide et obligations des entreprises](#).

OBLIGATIONS		EN PROCESSUS	FAIT
1	Avoir établi des politiques et des pratiques encadrant la gouvernance des renseignements personnels et <u>publier de l'information détaillée sur celles-ci en termes simples et clairs sur le site Internet de l'entreprise</u> ou, si elle n'a pas de site, par tout autre moyen approprié.	☐	☐
2	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 (guide d'accompagnement).	☐	☐
3	Respecter les nouvelles <u>règles entourant le consentement</u> à la collecte , à la communication ou à l'utilisation des renseignements personnels.	☐	☐
4	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.	☐	☐
5	Respecter vos nouvelles <u>obligations d'information et de transparence</u> envers les citoyens.	☐	☐
6	Respecter les nouvelles <u>règles de communication de renseignements personnels sans le consentement</u> de la personne concernée.	☐	☐

OBLIGATIONS		EN PROCESSUS	FAIT
7	Respecter les nouvelles <u>règles de communication des renseignements personnels à l'extérieur du Québec.</u>	☐	☐
8	Respecter les nouvelles règles d'utilisation des renseignements personnels.	☐	☐
9	Prévoir, par défaut, les paramètres assurant le plus haut niveau de confidentialité du produit ou du service technologique offert au public.	☐	☐
10	Respecter les nouvelles <u>règles entourant la collecte de renseignements personnels concernant un mineur.</u>	☐	☐
11	Respecter le <u>droit à la cessation de la diffusion, à la réindexation ou à la désindexation</u> (ou droit à l'oubli).	☐	☐
12	Respecter les nouvelles règles de <u>communication des renseignements personnels facilitant le processus de deuil.</u>	☐	☐

D'ici le 22 septembre 2024

Informez l'équipe responsable de l'entretien, de la mise à jour ou du développement de vos systèmes informatiques que vous avez de nouveaux besoins d'affaires en lien avec le droit à la portabilité des renseignements personnels, à savoir :

- que vos systèmes permettent de communiquer, sur demande d'une personne concernée, un renseignement personnel informatisé recueilli auprès d'elle, et ce, dans un format technologique structuré et couramment utilisé;
- que cette communication puisse également se faire à une personne ou à un organisme autorisé par la Loi à recueillir le renseignement, à la demande de la personne concernée.

À noter : Assurez-vous de **former votre personnel** pour qu'il développe les bons réflexes en matière de protection des renseignements personnels.

ANNEXE 1 : Faire l'inventaire des renseignements personnels : de quoi ça consiste ?

Cet exercice consiste à:

- faire l'inventaire de ce que l'on a (quels sont les renseignements que vous détenez sur autrui?);
- comprendre d'où ces données proviennent;
- savoir comment on les utilise et ce qu'on fait avec;
- répertorier là où on envoie ces données -vers quels tiers, etc.

Modèle de fichier pour tenir votre inventaire à jour.

ANNEXE 2 : Moyens de prévention

Modèle de politique de confidentialité (interne)

Modèle de politique de confidentialité (externe)

Modèle de politique de traitement des plaintes

Modèle de politique de conservation et destruction des dossiers

ANNEXE 3 : Plan de réponse

Modèle d'un plan de réponse aux incidents

Modèle de politique de confidentialité (voir l'Annexe B de la politique pour usage à l'interne)

ANNEXE 4 : Obligations de la technique biométrique

Information au sujet de la biométrie

Pour davantage d'information

Guide d'accompagnement

EVALUATION DES FACTEURS RELATIFS À LA VIE PRIVÉE

Guide Évaluation des facteurs relatifs à la vie privée

Modèle d'un rapport d'évaluation des facteurs relatifs à la vie privée

Pour davantage d'information

RÉFÉRENCES

[Document de la CDC d'Amos : Loi 25 résumé](#)

[Commission d'accès à l'information du Québec : entreprises privées](#)

[Gouvernement du Québec](#)

[Guide et obligations des entreprises](#)

[Blogue : De l'importance de dresser un inventaire des renseignements personnels dans votre organisation](#)

AUTRES OUTILS

[Informations en lien avec l'infonuagique](#)

[Procédure en cas d'incident](#)

EXEMPLE DE POLITIQUE DE CONFIDENTIALITÉ À AFFICHER SUR UN SITE INTERNET

[Politiques de confidentialité de la Commission d'accès à l'information du Québec](#)

[Politique de confidentialité de la Table nationale des CDC](#)

[Politique de confidentialité du ROCGIM-CDC](#)