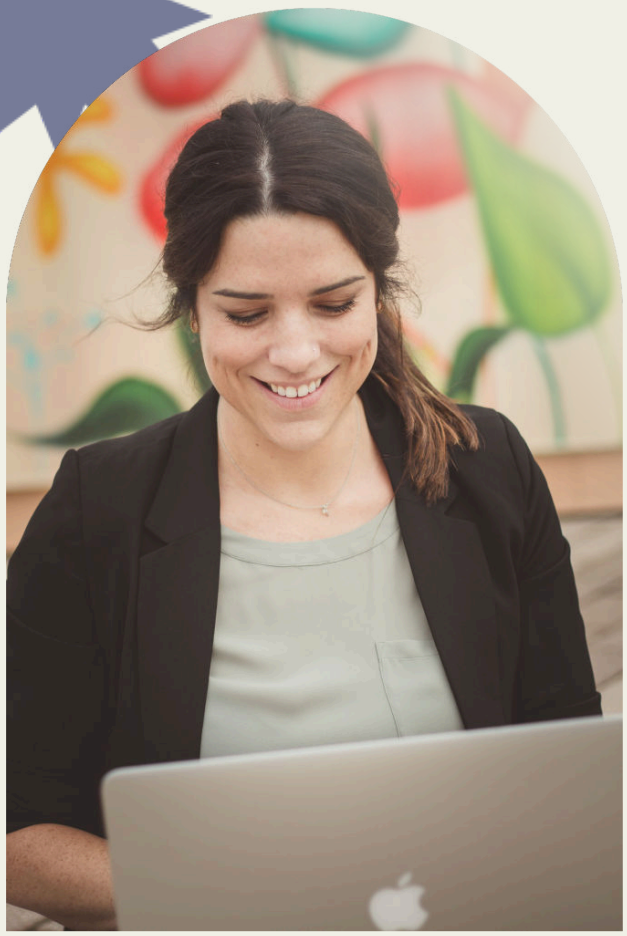
CHECKLIST

CONFORMITÉ LOI 25

MISE À JOUR AVRIL 2025



PF COMMUNICATIONS

Créé par: Patricia Filiatrault, PF communications

Checklist Loi 25

Je suis heureuse de te présenter notre liste de contrôle pour la Loi 25.

Celle-ci inclut les éléments de conformité mis en œuvre par PF communications ainsi que les meilleures pratiques pour t'aider à te conformer à la Loi 25. Garde en tête que ceci est seulement un aperçu et que la liste n'est pas exhaustive, mais donne un très bon portrait de tes obligations.

En cas de doute, consulte un avocat... parce que nous, nous ne sommes pas avocats, mais des experts Web. 😉

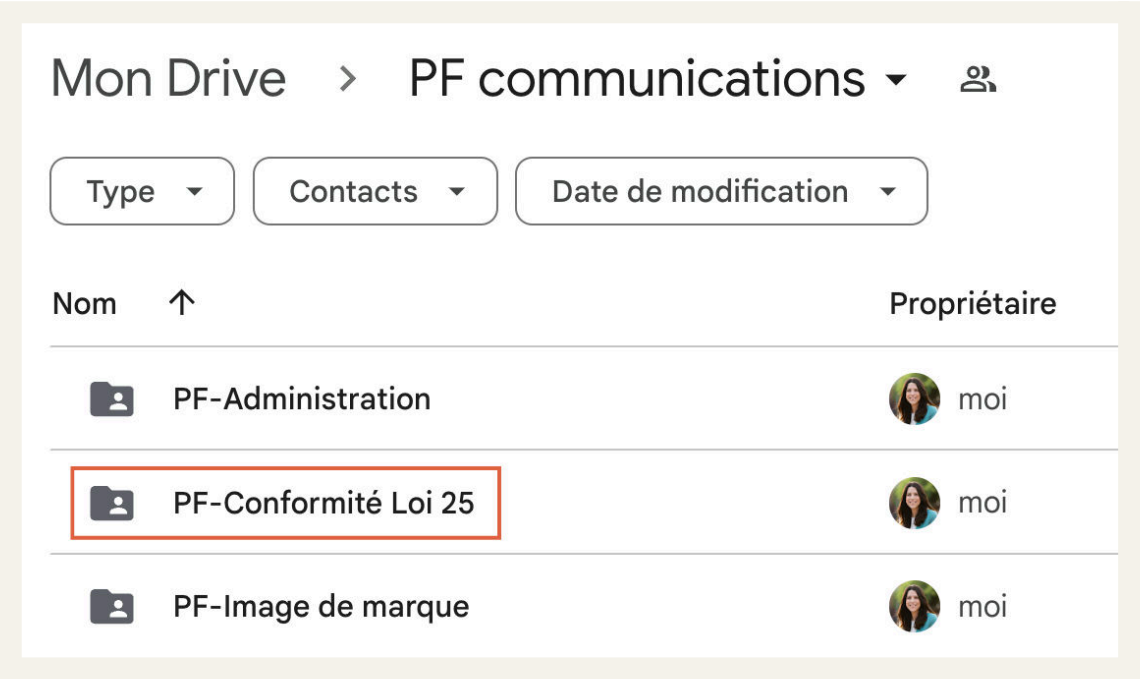
Savais-tu que...

Savais-tu que tous les sites Web récoltent des informations personnelles? Il suffit de penser à l'adresse IP des internautes qui naviguent sur un site.

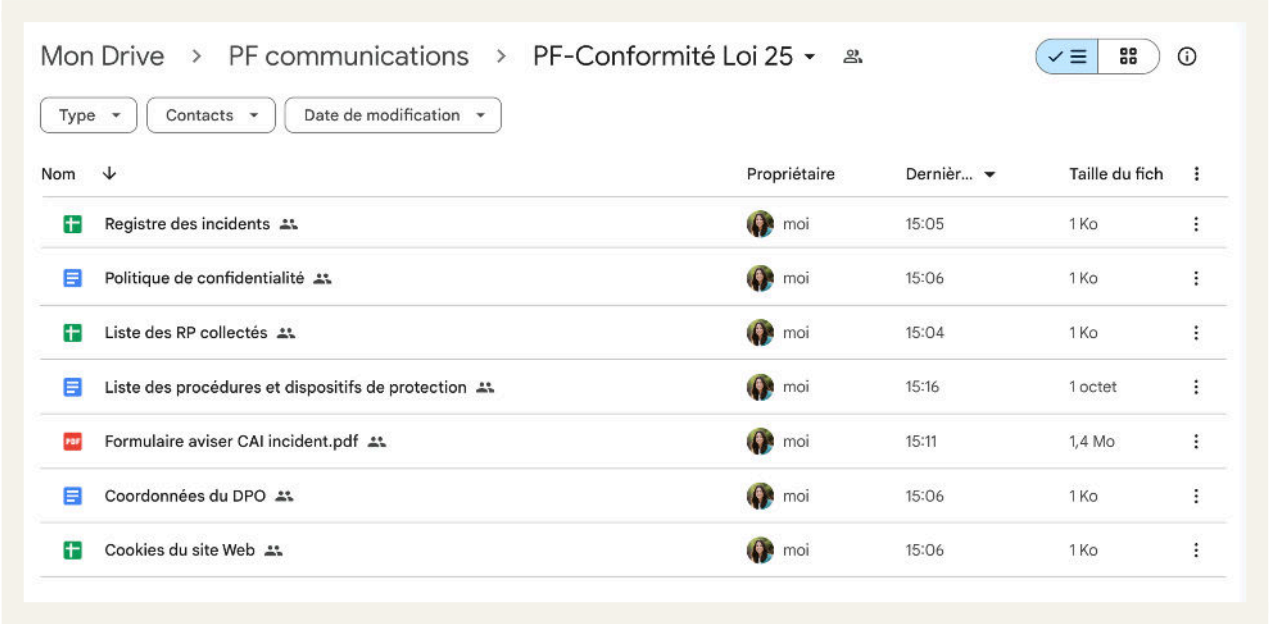
Ainsi, si tu possèdes un site, la Loi 25 te concerne directement!

Par où commencer?

Pour faciliter la gestion de la conformité à la Loi 25, crée un dossier sur Google Drive nommé **Nom de l'entreprise-Conformité Loi 25** où tu stockeras tous les documents pertinents. En cas de contrôle par le gouvernement, partage-leur ce dossier (de manière sécurisée évidemment). Psst... Il te faudra aussi leur prouver que tu obtiens les consentements pour les cookies de ton site Web (mais ça je t'en reparle plus loin dans le document).



Voici ce que contiendra notamment ce dossier :



Pour être conforme à la Loi 25, il te faut :

- ☐ **Lister les types de renseignements personnels (RP) que ton entreprise récolte sur ses clients, employés, collaborateurs, etc.** 📋
  Crée un document Google dans lequel tu dresseras un inventaire des RP recueillis. Exemples : nom, prénom, courriel, adresse IP, etc.

- ☐ **Déterminer une personne responsable de la protection des données (communément appelée Délégué à la protection des données – DPO).** 🙋
  Si tu es travailleur autonome, tu es le détenteur de cette responsabilité par défaut. Si l'entreprise ne nomme pas de DPO, ce sera automatiquement la personne ayant le plus haut niveau de responsabilité dans l'entreprise.

- ☐ **Divulguer les informations du DPO.** 📣
  Nous te suggérons d'indiquer l'identité et les coordonnées du DPO dans la section *Politique de confidentialité* sur ton site web.

☐ **Créer un registre des incidents de confidentialité.** 📋
Chaque incident compromettant la confidentialité d'une information personnelle doit être consigné dans un registre. Voici des exemples d'incidents :

- des informations confidentielles ont été envoyées à la mauvaise personne.
- un vol de cellulaire/ordinateur/disque externe.
- une attaque informatique (hameçonnage ou rançongiciel).

Pour chaque incident, documente les éléments suivants :

- la date à laquelle l'incident s'est produit
- la date de sa détection (le moment où tu as pris connaissance de l'incident)
- les circonstances de l'incident
- le nombre d'individus affectés
- les catégories des RP concernés.

Il est également important :

- d'indiquer si l'incident représente un préjudice sérieux,
- de préciser si et quand la Commission d'accès à l'information (CAI) a été notifiée,
- d'indiquer la date à laquelle les clients ont été informés de la situation,
- de détailler les mesures de sécurité implémentées pour prévenir un futur incident.

☐ **Divulguer les incidents de confidentialité.** ✏️
Comme tu as pu le comprendre au point précédent, lorsqu'un incident se produit, il est nécessaire d'en informer les parties concernées, soit la CAI (Commission d'accès à l'information du Québec) et la ou les personnes à qui appartiennent les renseignements.

- ☐ **Implémenter des dispositifs de protection.** 🔐
  Ton entreprise doit prouver qu'elle a adopté des mesures pour réduire les risques de divulgation et sécuriser les données personnelles. C'est crucial pour minimiser les pénalités potentielles de la Loi 25 (pouvant atteindre jusqu'à 50 000 $ pour les individus ou 4 % du chiffre d'affaires pour les entreprises).

  En pratique, cela signifie qu'en cas d'incident, il est essentiel de démontrer que des efforts ont été faits pour établir une solide sécurité informatique.

  Ceci dit, il est essentiel de démontrer **proactivement** que toutes les mesures nécessaires sont en place pour prévenir les incidents, même en l'absence de situations avérées. Autrement dit, il est crucial de maintenir une transparence et une rigueur constantes dans la gestion des risques.

  De plus, ton entreprise aura un gros plus avec toutes les preuves des consentements des cookies bien rangées grâce à la Plateforme de gestion du consentement (CMP en anglais) sur ton site.

- ☐ **Établir des règles de gestion des informations personnelles.** 🛑
  Il est nécessaire de mettre en place (et de respecter) des procédures régissant la gestion des données personnelles pour garantir leur sécurité au sein de ton entreprise.

  Par exemple, un pigiste engagé pour un projet déterminé ne devrait avoir accès qu'aux données relatives aux clients directement concernés par son travail, et uniquement aux informations indispensables à la réalisation de sa mission.

- ☐ **Afficher que tu collectes des renseignements confidentiels et informer de leur finalité.** 👍🏼
  Mentionne clairement aux personnes concernées les objectifs de la collecte, les moyens utilisés, ainsi que leurs droits d'accès, de modification et de retrait du consentement à tout moment. Indique les tiers receveurs ou partenaires de partage des données, comme PayPal ou Stripe.

  Ces informations doivent se retrouver dans ta politique de confidentialité et dans la bannière de consentement des cookies.

  La Loi 25 du Québec oblige les entreprises à expliquer pourquoi elles collectent des données personnelles. En gros, cela signifie que lorsque nous demandons des informations personnelles, nous devons dire exactement à quoi elles serviront. Cela protège la vie privée des gens, établit une relation de confiance et assure le respect de la loi.

☐ **Rendre tes politiques accessibles au public.** 👩‍🏫
Il est essentiel de diffuser tes politiques et tes pratiques, en utilisant un langage simple et compréhensible, sur ton site Web.

Par exemple, tu dois publier ta politique de confidentialité sur ton site Web.

Qu'est-ce que ça veut dire pour ton site Web?

Comme la Loi 25 le mentionne, ta politique de confidentialité doit être visible sur ton site Web. On la voit généralement dans le *footer* du site. Voici un exemple sur le site de PF communications.

☐ **Collecter seulement les informations indispensables.** ✅
Il est essentiel de limiter ta collecte aux données strictement nécessaires aux objectifs fixés avant à leur acquisition.

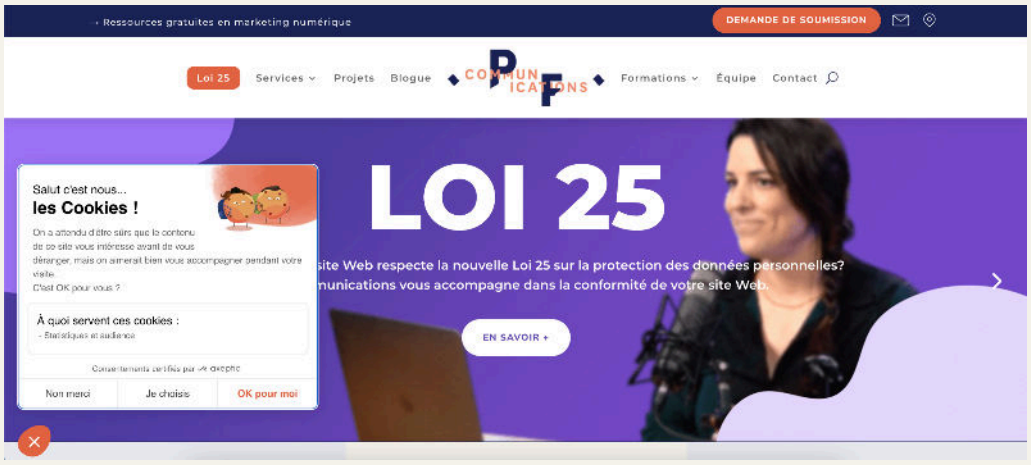
Exemple : demander la date et l'année de naissance pour un achat, ce n'est pas pertinent pour traiter une commande en ligne.

☐ **Obtenir l'accord avant la collecte.** 👌
Il est impératif de recueillir l'approbation des individus avant la collecte, l'utilisation, ou la divulgation de leurs données personnelles.

Qu'est-ce que ça veut dire pour ton site Web?

Même si la Loi ne dit pas comment le faire, la pratique est de mettre en place un popup qui informera tes visiteurs quant à la collecte de données. Ils devront accepter ou non que leurs données soient récoltées.

Attention. Mettre un popup ne suffit pas. Il doit être connecté à ton Google Tag Manager afin d'activer ou de bloquer la collecte de données.



- ☐ **Fournir les informations détenues sur sollicitation.** 👉
  Si tu détiens des informations personnelles sur une personne, tu dois, à sa demande, lui confirmer l'existence de ces informations et lui fournir une copie de celles-ci.

- ☐ **Effacer des données à la demande d'un individu (droit à l'oubli).** 🚫
  Une personne peut demander à une entreprise de supprimer un renseignement personnel qu'elle détient à son sujet.

- ☐ **Éliminer (ou anonymiser) les données** 🗑️
  Tu es tenu de supprimer toute information personnelle collectée il y a plus de 7 ans. Des exceptions s'appliquent.

Bonnes pratiques pour te conformer à la Loi 25

Pour respecter les exigences de la Loi 25, plusieurs bonnes pratiques sont de rigueur. En voici quelques-unes.

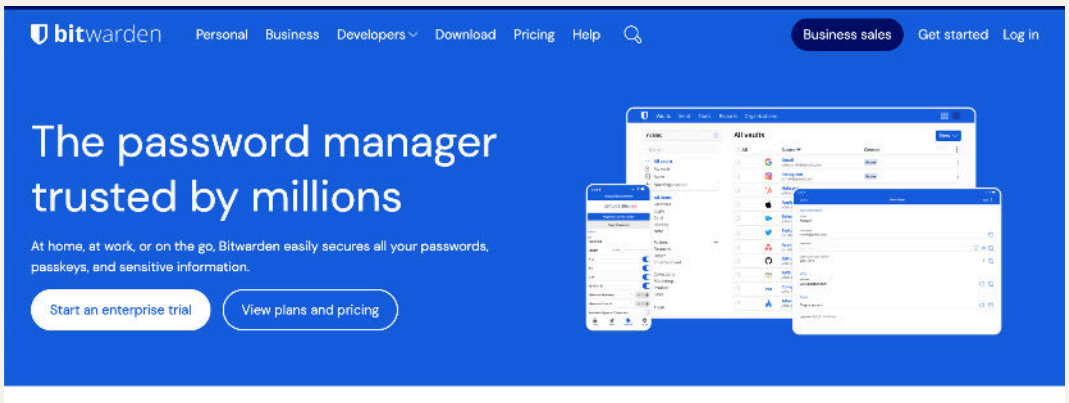
- ☐ **Mots de passe forts (12 caractères et plus)** 🔒

- ☐ **Installer un antivirus sur les ordinateurs de ton entreprise.** 🖥️

- ☐ **Établir un système de protection des mots de passe qui circulent dans ton entreprise.** 🔄

Qu'est-ce que ça veut dire pour ton entreprise ?

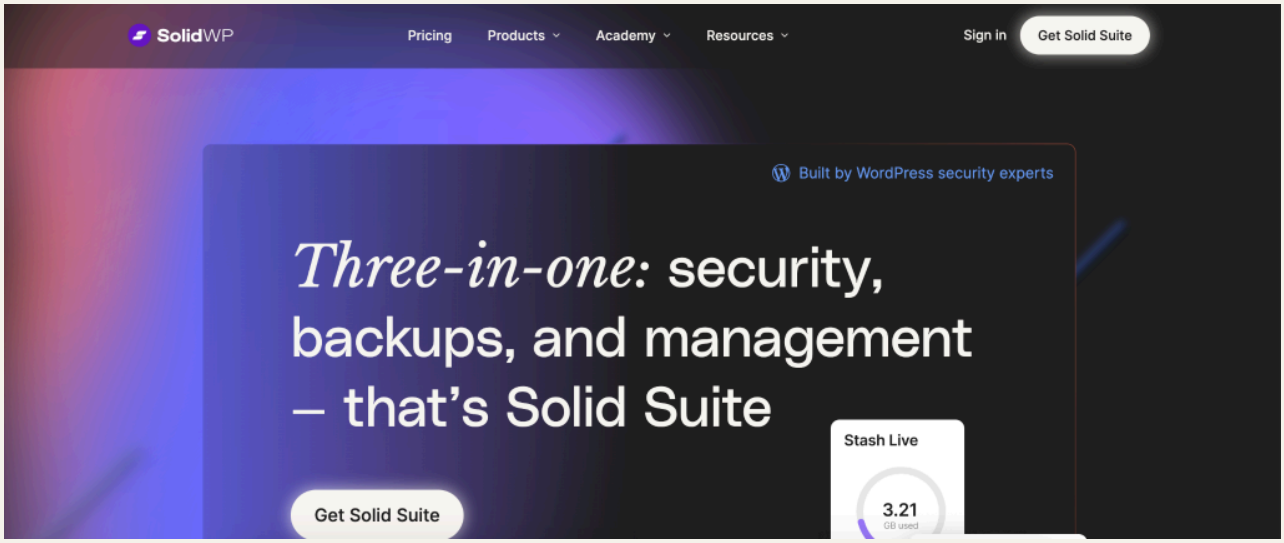
Les mots de passe, ce n'est jamais facile à gérer, surtout si tu as des employés ou que tu travailles avec des pigistes. Pour augmenter la sécurité entourant le partage des mots de passe, tu peux utiliser un logiciel de gestion des mots de passe. Il en existe plusieurs. Chez PF communications, nous avons choisi Bitwarden.



- ☐ **Mettre en place l'authentification à deux facteurs là où c'est disponible.** 💻
- ☐ **Mettre à jour les applications et les extensions que tu utilises, particulièrement en cas de publication d'une mise à jour faisant suite à une faille de sécurité identifiée.** ⚙️
- ☐ **Protéger efficacement ton site internet.** 🥽

Qu'est-ce que ça veut dire pour ton site Web?

Chez PF communications, nous optons pour le plugin ITheme Security pour WordPress, maintenant appelé SolidWP. SolidWP permet, entre autres, de faire des mises à jour et protéger ton site Web.



- ☐ **Effectuer régulièrement des sauvegardes des données.** 💾
- ☐ **Assurer la sauvegarde des fichiers stockés sur des solutions cloud.** ☁️
- ☐ **Limiter l'usage de supports amovibles (disques durs externes, clés USB, etc.) pour éviter pertes et vols.** 💿
- ☐ **Utiliser une adresse courriel professionnelle avec ton propre nom de domaine (ex. : prenom@tonentreprise.com) plutôt qu'une adresse générique et gratuite (gmail.com, hotmail.com, etc.).**
- ☐ **Créer des courriels alias pour tes logiciels.**

En utilisant des courriels alias, tu t'assureras que les courriels reçus proviennent bien du logiciel en question et non d'un site malveillant.
Exemple : entreprise+logiciel@domaine.ca ✉️

☐ **Héberger son site au Québec.** 🏠
Je te recommande Likuid.

Anonymisation des données et conformité à la Loi 25

La Loi 25 exige la destruction des renseignements personnels une fois leur utilisation terminée. Cependant, elle offre aussi une alternative intéressante depuis 2024 : l'anonymisation des données.

L'anonymisation permet de conserver certaines informations pour des analyses stratégiques sans compromettre la vie privée des individus. Elle consiste à retirer tout élément permettant d'identifier une personne, de manière irréversible.

Voici quelques étapes clés pour anonymiser des données selon la Loi 25 :

✅ **Suppression des identifiants directs** : Retirer les noms, adresses courriel, numéros de téléphone et toute autre donnée pouvant identifier directement un individu.

Évaluation du risque de réidentification : Vérifier si les données restantes peuvent encore permettre d'identifier quelqu'un en croisant des informations.

Application de techniques d'anonymisation :

- **Ajout de bruit** : Modifier légèrement les valeurs pour empêcher l'identification.
- **Permutation** : Mélanger les données entre différents individus pour brouiller les pistes.
- **Agrégation** : Regrouper les informations sous des catégories plus larges (ex.: un âge exact devient une tranche d'âge).

Vérification finale : S'assurer que les données ne permettent plus d'identifier une personne, même indirectement.

✅ **Documentation obligatoire** : Depuis janvier 2025, un registre d'anonymisation doit être tenu, incluant les techniques utilisées et les analyses de risque effectuées.

L'anonymisation est un excellent moyen de respecter la Loi 25 tout en continuant à utiliser des données à des fins légitimes, comme le suivi marketing et l'amélioration des services.

Audit initial et suivi régulier

- Planifier un audit initial pour évaluer la conformité actuelle de votre entreprise à la Loi 25.
- Mettre en place un suivi périodique (tous les 6 ou 12 mois) pour s'assurer que les pratiques restent conformes.
- Utiliser une checklist de suivi et documenter toute mise à jour des pratiques.

Formation et sensibilisation des employés

- Offrir une formation obligatoire sur la protection des données personnelles à tous les employés.
- Créer un guide interne de bonnes pratiques en gestion des données personnelles.
- Sensibiliser les équipes à l'importance de la confidentialité et à la Loi 25.

Droits des utilisateurs et gestion des demandes

- Établir un processus clair pour répondre aux demandes d'accès, de modification ou de suppression des données personnelles.
- Désigner une personne responsable du traitement des demandes (DPO ou responsable désigné).
- Documenter toutes les demandes et les délais de traitement.

Protection avancée des données

- Activer le chiffrement des bases de données et des fichiers contenant des informations sensibles.
- Vérifier que les outils cloud utilisés sont conformes aux réglementations sur la protection des données.
- Restreindre les accès aux données sensibles à seulement ceux qui en ont besoin.

Gestion des sous-traitants et des tiers

- Vérifier que vos fournisseurs et partenaires respectent aussi la Loi 25.
- Faire signer des clauses contractuelles de conformité à la Loi 25 aux prestataires qui traitent des données personnelles.
- Exiger des garanties de sécurité et de confidentialité de la part des sous-traitants.

Documentation et archivage des preuves de conformité

- Conserver des preuves des actions mises en place (politiques internes, logs de sécurité, rapports d'audit, etc.).
- Mettre en place une procédure de mise à jour régulière de ces documents.
- Centraliser tous les documents dans un dossier sécurisé pour faciliter les contrôles éventuels.

As-tu besoin d'aide?

Maintenant que tu as une meilleure vue sur la Loi 25? Te sens-tu plus outillé.e pour commencer à mettre en place le nécessaire dans ton entreprise?

Je te laisse quelques jours pour commencer à implanter quelques premières étapes. Si certains éléments te semblent nébuleux pour ton site Web, l'équipe de PF communications est prête à t'accompagner. Écris-moi au pf@patriciafiliatrault.com.

C'EST UN *plaisir* DE TRAVAILLER AVEC TOI !

PF communications Inc.
228 Rue Champlain
Saint-Jean-sur-Richelieu, QC J3B 6V8
514 756-6869 | pf@patriciafiliatrault.com