CPA COMPTABLES PROFESSIONNELS AGRÉÉS

20 MINUTES cpa

COMPRENDRE LA LOI 25 EN 20 MINUTES

Carl Robillard, CPA, M.Sc.
Conseils Strateg-TI

COMPRENDRE LA LOI 25

La Loi 25 en bref

Les éléments de conformité

Atelier pratique

Prochaines étapes

Le matériel ne peut être reproduit, modifié ou imprimé sans autorisation, en tout ou en partie, sous quelque forme et par quelque moyen que ce soit (électroniquement, mécaniquement, par photocopie, enregistrement ou toute autre méthode, y compris sa diffusion sur un réseau informatique privé ou public)

La Loi 25 en bref



Le matériel ne peut être reproduit, modifié ou imprimé sans autorisation, en tout ou en partie, sous quelque forme et par quelque moyen que ce soit (électroniquement, mécaniquement, par photocopie, enregistrement ou toute autre méthode, y compris sa diffusion sur un réseau informatique privé ou public).

La Loi 25 en bref

«3.2. Toute personne qui exploite une entreprise doit établir et mettre en œuvre des politiques et des pratiques encadrant sa gouvernance à l'égard des renseignements personnels et propres à assurer la protection de ces renseignements.

Celles-ci doivent notamment prévoir l'encadrement applicable à la conservation et à la destruction de ces renseignements, prévoir les rôles et les responsabilités des membres de son personnel tout au long du cycle de vie de ces renseignements et un processus de traitement des plaintes relatives à la protection de ceux-ci.

Elles doivent également être proportionnées à la nature et à l'importance des activités de l'entreprise et être approuvées par le responsable de la protection des renseignements personnels. ...»

Le matériel ne peut être reproduit, modifié ou imprimé sans autorisation, en tout ou en partie, sous quelque forme et par quelque moyen que ce soit (électroniquement, mécaniquement, par photocopie, enregistrement ou toute autre méthode, y compris sa diffusion sur un réseau informatique privé ou public)

Que devez-vous protéger?

Renseignements personnels

Les renseignements personnels sont ceux qui portent sur une personne physique et permettent de l'identifier. Ils doivent demeurer confidentiels. Sauf exception, ils ne peuvent être communiqués sans le consentement de la personne concernée.

Renseignements sensibles

Désigne des renseignements personnels qui, par leur nature notamment médicale, biométrique, financière ou autrement intime, ou en raison du contexte de son utilisation ou de sa communication, suscitent un haut degré d'attente raisonnable en matière de vie privée (ex: orientation sexuelle, allégeance politique, etc).

Le matériel ne peut être reproduit, modifié ou imprimé sans autorisation, en tout ou en partie, sous quelque forme et par quelque moyen que ce soit (électroniquement, mécaniquement, par photocopie, enregistrement ou toute autre méthode, y compris sa diffusion sur un réseau informatique privé ou public)

Objectif de la Loi 25

Renforcer la protection des renseignements personnels d'une personne physique, afin de prévenir et de contrer le vol d'identité, la fraude ou une atteinte à la réputation de celle-ci.

Les entreprises doivent démontrer leur engagement et agir de façon diligente dans la mesure de leurs moyens.

Le matériel ne peut être reproduit, modifié ou imprimé sans autorisation, en tout ou en partie, sous quelque forme et par quelque moyen que ce soit (électroniquement, mécaniquement, par photocopie, enregistrement ou toute autre méthode, y compris sa diffusion sur un réseau informatique privé ou public)

Loi 25 : progressive et « ferme »

3 phases, quelques exigences et les impacts *

Communication

Phase 1 : 22 septembre 2022

- Avoir « 1 » responsable
- Mise en place d'un comité
- Obligation d'informer en cas d'incident
- Nouvel encadrement de la communication des renseignements personnels

Rigueur

Phase 2 : septembre 2023

- Obligation de mettre en œuvre des politiques et des pratiques encadrant la gouvernance des renseignements personnels
- Nouvelles obligations de transparence
- Obligation de réaliser une évaluation des facteurs relatifs à la vie privée dans certaines situations

Outils et plan

Phase 3 : septembre 2024

Le droit à la portabilité sera la disposition finale à entrer en vigueur, autant dans le secteur public que dans le secteur privé. Cette obligation aura une incidence sur des changements structurels de la part des organisations. Mieux vaut y penser maintenant... et surtout, agir.

En cas de problème

Sanction dès septembre 2023

Sanctions administratives :

- Personne : jusqu'à 50 000 $
- Entreprise : 2 % du CA mondial, max. 10 M$

Poursuites pénales

- Personne : jusqu'à 100 000 $
- Entreprise : 4 % du CA mondial, max. 25 M$

Sources : Divers sites gouvernementaux du Québec / *Informations partielles seulement. Ce tableau est un aperçu non exhaustif.

Le matériel ne peut être reproduit, modifié ou imprimé sans autorisation, en tout ou en partie, sous quelque forme et par quelque moyen que ce soit (électroniquement, mécaniquement, par photocopie, enregistrement ou toute autre méthode, y compris sa diffusion sur un réseau informatique privé ou public)

Cycle de vie d'un renseignement personnel



Obligations

Collecte	Utilisation	Communication	Conservation	Destruction
- Déterminer le but - Limiter la collecte - Consentement	- Limiter l'accès - Limiter l'utilisation	- Consentement	- Assurer la qualité - Assurer l'intégrité	- Détruire dans les délais

Le matériel ne peut être reproduit, modifié ou imprimé sans autorisation, en tout ou en partie, sous quelque forme et par quelque moyen que ce soit (électroniquement, mécaniquement, par photocopie, enregistrement ou toute autre méthode, y compris sa diffusion sur un réseau informatique privé ou public)

Les éléments de conformité



Le matériel ne peut être reproduit, modifié ou imprimé sans autorisation, en tout ou en partie, sous quelque forme et par quelque moyen que ce soit (électroniquement, mécaniquement, par photocopie, enregistrement ou toute autre méthode, y compris sa diffusion sur un réseau informatique privé ou public)

Désignation du responsable

La personne ayant la plus haute autorité dans l'entreprise est par défaut responsable de la protection des renseignements personnels et se doit s'assurer le respect et la mise en œuvre de la Loi.

Ses responsabilités

- **Approuver les politiques et pratiques**
- **Recevoir les demandes et y répondre** (accès, rectification, cessation de diffusion, désindexation, réindexation, etc.) et être en mesure de **justifier les refus**.
- **Interlocuteur auprès de la Commission d'accès à l'information**
- **Documenter les incidents** (enregistrer les communications susceptibles de diminuer le risque, évaluation du préjudice etc.)
- Prend part à **l'évaluation des facteurs relatifs à la vie privée**.
- **Répondre aux demandes** des personnes concernant le droit à la portabilité (2024).



Le matériel ne peut être reproduit, modifié ou imprimé sans autorisation, en tout ou en partie, sous quelque forme et par quelque moyen que ce soit (électroniquement, mécaniquement, par photocopie, enregistrement ou toute autre méthode, y compris sa diffusion sur un réseau informatique privé ou public)

Étapes de la conformité

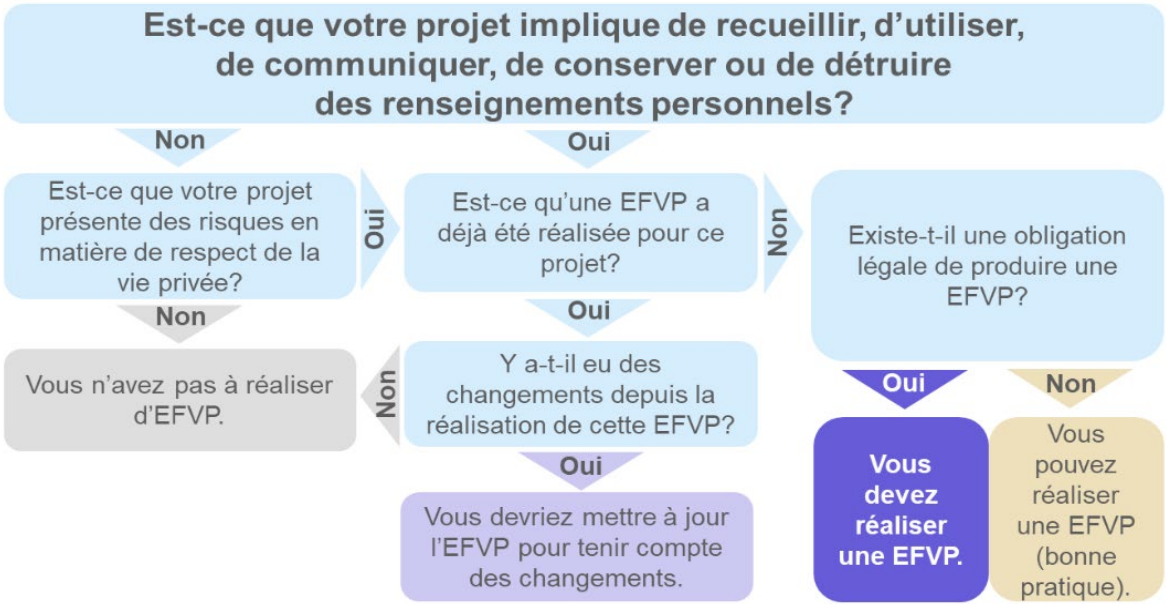
- Établir les politiques de protection des renseignements personnels*
- Processus de consentement pour collecte, détention et utilisation
- Processus de conservation, destruction et anonymisation
- Registre des incidents
- Processus de demande de correction et de désindexation
- Processus d'évaluation des facteurs relatifs à la vie privée (EFVP)
- Processus de notification des incidents
- Processus de traitement des plaintes*
- Mesures de portabilité (2024)

*Doivent être publiés sur le site web de l'entreprise

Le matériel ne peut être reproduit, modifié ou imprimé sans autorisation, en tout ou en partie, sous quelque forme et par quelque moyen que ce soit (électroniquement, mécaniquement, par photocopie, enregistrement ou toute autre méthode, y compris sa diffusion sur un réseau informatique privé ou public)

Évaluation des facteurs relatifs à la vie privée

À faire si vous avez un nouveau logiciel en vue



Le matériel ne peut être reproduit, modifié ou imprimé sans autorisation, en tout ou en partie, sous quelque forme et par quelque moyen que ce soit (électroniquement, mécaniquement, par photocopie, enregistrement ou toute autre méthode, y compris sa diffusion sur un réseau informatique privé ou public)

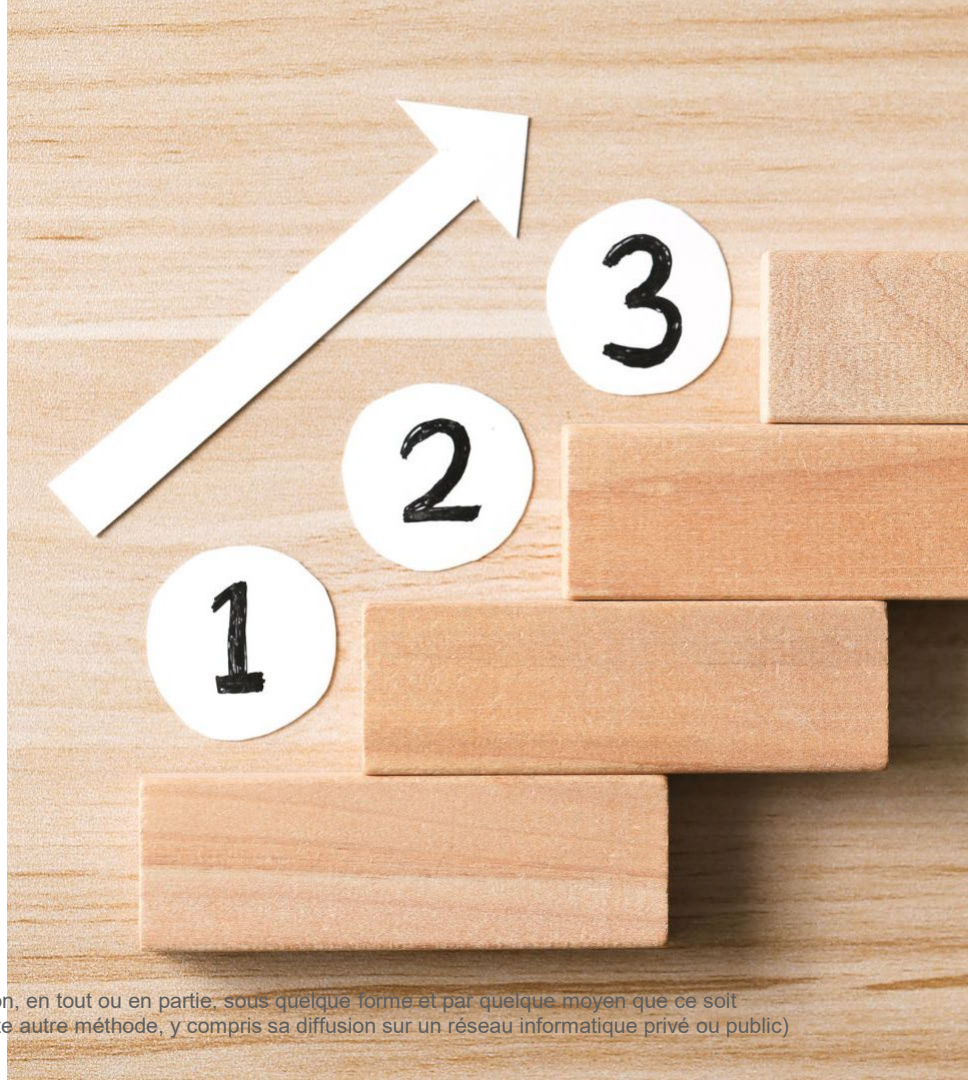
Atelier pratique



> Tableaux Excel

Le matériel ne peut être reproduit, modifié ou imprimé sans autorisation, en tout ou en partie, sous quelque forme et par quelque moyen que ce soit (électroniquement, mécaniquement, par photocopie, enregistrement ou toute autre méthode, y compris sa diffusion sur un réseau informatique privé ou public)

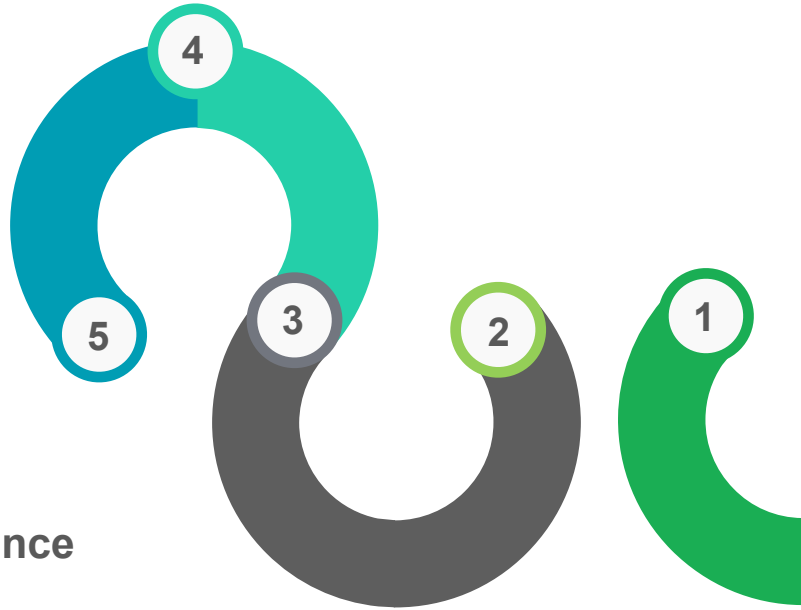
Prochaines étapes



Le matériel ne peut être reproduit, modifié ou imprimé sans autorisation, en tout ou en partie, sous quelque forme et par quelque moyen que ce soit (électroniquement, mécaniquement, par photocopie, enregistrement ou toute autre méthode, y compris sa diffusion sur un réseau informatique privé ou public)

Les étapes

1. **Inventaire des applications et registre des renseignements**
2. **Préparation des politiques**
3. **Préparation des formulaires**
4. **Analyse entre votre position actuelle en matière de gouvernance et celle à viser**
5. **Formation : Mettre en opération la gouvernance de la Loi 25 et la gérer au quotidien**



Le matériel ne peut être reproduit, modifié ou imprimé sans autorisation, en tout ou en partie, sous quelque forme et par quelque moyen que ce soit (électroniquement, mécaniquement, par photocopie, enregistrement ou toute autre méthode, y compris sa diffusion sur un réseau informatique privé ou public)

Pour plus de conseils et outils :

20minutescpa.ca

Ou suivez-nous sur LinkedIn



20 MINUTES cpa

Carl Robillard, CPA
Conseils Strateg-TI

Pour télécharger cette présentation et les outils proposés

Le matériel sera disponible durant une semaine.

Annexes



Le matériel ne peut être reproduit, modifié ou imprimé sans autorisation, en tout ou en partie, sous quelque forme et par quelque moyen que ce soit (électroniquement, mécaniquement, par photocopie, enregistrement ou toute autre méthode, y compris sa diffusion sur un réseau informatique privé ou public)

Protection des données

- ☐ Avez-vous suivi avec vos employés une formation sur les pratiques exemplaires en matière de cybersécurité?
- ☐ Des lignes directrices, des règlements et des directives en matière de cybersécurité sont-ils en place?
- ☐ Exigez-vous des mots de passe complexes et uniques?
- ☐ Exigez-vous une authentification à facteurs multiples pour accéder aux applications, aux services, etc.?
- ☐ Avez-vous mis en place des mises à jour automatiques et des correctifs pour les logiciels et le matériel?
- ☐ Utilisez-vous seulement des médias portatifs sécurisés qui appartiennent à votre organisation?
- ☐ Des logiciels antivirus et antimaliciels sont-ils installés sur vos appareils?
- ☐ Sauvegardez-vous les renseignements essentiels de votre entreprise de façon régulière?
- ☐ Disposez-vous de copies de sauvegarde chiffrées que vous avez testées?

Le matériel ne peut être reproduit, modifié ou imprimé sans autorisation, en tout ou en partie, sous quelque forme et par quelque moyen que ce soit (électroniquement, mécaniquement, par photocopie, enregistrement ou toute autre méthode, y compris sa diffusion sur un réseau informatique privé ou public)

Cybersécurité : l'harmonie entre 4 piliers






Éducation	Prévention	Détection	Récupération
Des lignes directrices, des règlements et des directives en matière de cybersécurité sont-ils en place? Sont-ils compris et mis en œuvre par tout le personnel?	Avez-vous déterminé les renseignements essentiels de votre entreprise? Exigez-vous une authentification à facteurs multiples pour accéder aux applications, aux services…?	Des logiciels antivirus et antimaliciels sont-ils installés sur vos appareils? Disposez-vous d'un plan d'intervention en cas d'incident et d'un plan de continuité des activités que vous avez testés?	Sauvegardez-vous les renseignements essentiels de votre entreprise de façon régulière? Disposez-vous de copies de sauvegarde chiffrées que vous avez testées?

Source : CyberSécuritaire Canada à canada.ca/CyberSecure / *Informations partielles seulement. Ce tableau est un aperçu non exhaustif.

Le matériel ne peut être reproduit, modifié ou imprimé sans autorisation, en tout ou en partie, sous quelque forme et par quelque moyen que ce soit (électroniquement, mécaniquement, par photocopie, enregistrement ou toute autre méthode, y compris sa diffusion sur un réseau informatique privé ou public)