

 CYBERSÉCURITÉ · GOUVERNANCE · CONFORMITÉ

La Loi 25 expliquée simplement

Le guide essentiel des PME québécoises pour comprendre leurs obligations, gagner la confiance de leurs clients et réduire leurs risques.

7 obligations décryptées

Auto-évaluation incluse

Modèles & procédures

VN

Virgile Landry Nguegnia, M. Sc., CISSP

Conseiller senior en sécurité de l'information · NB Solution inc.

NB Solution inc.

www.nbsolution.link · 418-800-2030

Pourquoi ce guide vous **concerne**

Si votre entreprise possède une liste de clients, un site Web, un formulaire de contact, une infolettre ou simplement des dossiers employés, vous êtes très probablement assujéti à la Loi 25.

« La conformité à la Loi 25 n'est pas qu'une obligation légale : c'est un investissement dans la confiance de vos clients. »

La bonne nouvelle ? La majorité des PME peuvent atteindre un bon niveau de conformité avec quelques actions structurées. Ce guide a été conçu pour vous aider à **comprendre vos obligations** et à **identifier rapidement les premières actions** à mettre en place — sans jargon inutile.

À QUI S'ADRESSE CE GUIDE



Entrepreneurs

Travailleurs autonomes et dirigeants de PME.



Commerces & services

Détail, services professionnels et cabinets.



Manufacturiers

PME industrielles et organisations en croissance.



Virgile Landry Nguegnja, M. Sc., CISSP

Conseiller senior en sécurité de l'information — accompagne les PME québécoises dans leur mise en conformité à la Loi 25 et leur posture de cybersécurité.

CERTIFIÉ CISSP

Ce que vous allez découvrir

PARTIE 1 — COMPRENDRE LA LOI 25

01	La Loi 25 en quelques mots	05
02	Votre entreprise est-elle concernée ?	06
03	Qu'est-ce qu'un renseignement personnel ?	07

PARTIE 2 — VOS OBLIGATIONS

04	Les 7 obligations incontournables	09
05	Le consentement valide	10
06	Les sanctions prévues par la loi	11

PARTIE 3 — PASSER À L'ACTION

07	Les erreurs les plus fréquentes	13
08	Le calendrier de conservation	14
09	Le registre des incidents	15
10	Les procédures essentielles	16
11	Auto-évaluation de votre maturité	17

PARTIE 4 — ALLER PLUS LOIN

12	Comment NB Solution vous accompagne	19
13	Votre diagnostic gratuit	20

01

PARTIE 1

Comprendre la Loi 25

Avant d'agir, il faut comprendre. Cette partie pose les bases : ce qu'est la Loi 25, si votre entreprise est concernée, et ce que recouvre vraiment la notion de « renseignement personnel ».

- 01 La Loi 25 en quelques mots
- 02 Votre entreprise est-elle concernée ?
- 03 Qu'est-ce qu'un renseignement personnel ?

La Loi 25 en quelques mots

La Loi 25 modernise les règles québécoises en matière de protection des renseignements personnels. Son objectif : offrir aux citoyens un meilleur contrôle sur leurs données et amener les organisations à adopter de meilleures pratiques.



Objectif principal

Protéger la confidentialité des renseignements personnels et garantir leur traitement adéquat tout au long de leur cycle de vie.



Portée d'application

Toute organisation qui exerce des activités au Québec et qui collecte des renseignements personnels — quelle que soit sa taille.



Nouveaux droits citoyens

Consentement clair, droit à l'oubli (désindexation), portabilité des données et obligation d'évaluation (ÉFVP).



Des sanctions réelles

Le non-respect peut entraîner des pénalités importantes — détaillées au chapitre 6.



L'esprit de la loi en une phrase

La Loi 25 redonne au citoyen le contrôle de ses renseignements personnels — et fait de leur protection une responsabilité partagée par toutes les organisations.

Votre entreprise **est-elle concernée ?**

Répondez par OUI ou NON aux affirmations suivantes. Une seule réponse positive suffit : votre entreprise traite probablement des renseignements personnels.

☐ J'ai un site Web.

☐ J'ai un formulaire de contact.

☐ Je collecte des courriels.

☐ Je possède des dossiers employés.

☐ Je prends des rendez-vous en ligne.

☐ J'utilise Facebook ou LinkedIn pour générer des prospects.

☐ J'utilise Excel ou un CRM pour mes clients.

☐ Je fais des factures.



Une seule case suffit.

Si vous avez répondu OUI à une seule de ces affirmations, la Loi 25 s'applique à vous. La quasi-totalité des PME québécoises sont concernées.

Qu'est-ce qu'un **renseignement personnel** ?

C'est tout renseignement qui permet d'identifier une personne physique, **directement ou indirectement**. On peut les regrouper en cinq grandes familles.

1



Ce qui me décrit

Nom, numéro d'assurance maladie, photographie, empreintes, origine ethnique, langue maternelle, identité de genre, renseignements médicaux.

2



Mes coordonnées

Adresse IP, adresse courriel, adresse postale, numéro de téléphone, position GPS.

3



Mon portefeuille

Numéro de carte de crédit, achats effectués, nombre de prêts, dossier de crédit, possessions matérielles (maison, automobile).

4



Ce que je pense

Croyances, opinions, intentions, plats favoris, intérêts, mots de passe choisis.

5



Ma vie en communauté

Réputation, statut marital, type de famille, liste d'amis Facebook, historique d'appels, curriculum vitæ, condamnations.



Renseignements sensibles

Santé, origine, opinions politiques, données biométriques : ils exigent un **consentement exprès** et une vigilance accrue.

02

PARTIE 2

Vos obligations

Sept obligations structurent la conformité à la Loi 25. Voici ce que la loi attend concrètement de votre entreprise — du consentement aux sanctions encourues.

- 04 Les 7 obligations incontournables
- 05 Le consentement valide
- 06 Les sanctions prévues par la loi

Les 7 obligations **incontournables**

Ces sept piliers forment le socle de la conformité. La plupart sont accessibles à une PME avec un accompagnement structuré.

01



Désigner un responsable

Nommer un responsable de la protection des renseignements personnels.

02



Politique de confidentialité

Publier une politique claire et accessible à vos clients.

03



Consentement valide

Obtenir un consentement libre, éclairé et à des fins précises.

04



Gérer les incidents

Tenir un registre et un processus de notification des incidents.

05



Détruire les données

Supprimer les renseignements lorsqu'ils ne sont plus nécessaires.

06



Réaliser une ÉFVP

Évaluer les facteurs relatifs à la vie privée pour les nouveaux projets.

07



Former les employés

Sensibiliser les équipes aux bonnes pratiques et aux risques.

Par où commencer ?

Un diagnostic identifie les 2-3 obligations prioritaires pour votre entreprise.

Le consentement valide

Le consentement est l'autorisation qu'une personne accorde pour permettre à une organisation de collecter, utiliser ou communiquer ses renseignements personnels. Pour être valide, il doit réunir quatre qualités.

Manifeste

Donné de façon claire et non équivoque
— jamais présumé ni caché dans de longues conditions.

Libre

Accordé sans contrainte : la personne doit pouvoir refuser sans conséquence injustifiée.

Éclairé

Formulé en termes simples et clairs, en sachant à quoi l'on consent.

Spécifique

Demandé pour chacune des fins visées, et limité dans le temps.

— LES RÈGLES D'OR

- ✓ Le consentement est demandé **pour chaque finalité** , en termes simples et clairs.
- ✓ Par écrit, il est présenté **distinctement** de toute autre information.
- ✓ Un renseignement ne peut servir à une **autre fin** sans nouveau consentement.
- ✓ Les renseignements **sensibles** exigent un consentement formulé expressément.



En pratique

Une case pré-cochée ou un consentement « groupé » pour plusieurs finalités n'est pas valide. Séparez clairement chaque demande.

Les sanctions prévues par la loi

Au-delà du risque financier, l'enjeu le plus important pour une PME reste souvent la perte de confiance des clients. Mais les sanctions administratives sont, elles, bien réelles.

10 M\$

Sanction maximale (autres cas)

2 %

... ou du chiffre d'affaires mondial, si plus élevé

50 000 \$

Maximum pour une personne physique

Catégorie	Pers. physique — base	Pers. physique — max	Autres cas — base	Autres cas — max
A	500 \$	50 000 \$	1 000 \$	10 M\$ / 2 %
B	1 500 \$	50 000 \$	4 000 \$	10 M\$ / 2 %
C	3 000 \$	50 000 \$	8 000 \$	10 M\$ / 2 %
D	5 000 \$	50 000 \$	15 000 \$	10 M\$ / 2 %

« Autres cas » : personnes morales, sociétés en nom collectif et sociétés en commandite. Le montant maximal correspond à 10 M\$ ou 2 % du chiffre d'affaires mondial de l'exercice précédent, selon le plus élevé.



Le vrai risque pour une PME

Une plainte d'un client, une fuite de données, une atteinte à la réputation ou une demande d'accès à laquelle l'entreprise ne sait pas répondre — souvent plus probable qu'une amende maximale.

03

PARTIE 3

Passer à l'action

La théorie ne protège personne. Cette partie vous donne des outils concrets : erreurs à éviter, calendrier de conservation, modèle de registre, procédures et une auto-évaluation de votre maturité.

- 07 Les erreurs les plus fréquentes
- 08 Le calendrier de conservation
- 09 Le registre des incidents
- 10 Les procédures essentielles
- 11 Auto-évaluation de votre maturité

Les erreurs les plus fréquentes

Aucune mauvaise intention derrière ces erreurs — juste des habitudes. Les reconnaître est déjà un grand pas vers la conformité.



Compte personnel pour les affaires

Utiliser un Gmail personnel pour les communications professionnelles.



Conserver les CV trop longtemps

Garder des candidatures pendant des années sans justification.



Partage via apps non contrôlées

Transférer des fichiers clients par Messenger ou WhatsApp personnel.



Ne pas savoir où sont les données

Ignorer dans quels outils et lieux les renseignements sont stockés.



Accès non désactivés

Laisser partir un employé sans révoquer ses accès aux systèmes.



Copie sur un ordinateur personnel

Dupliquer une base clients sur un appareil non sécurisé.



La bonne nouvelle

Chacune de ces erreurs se corrige avec une politique claire, des outils adaptés et un peu de sensibilisation — sans bouleverser votre fonctionnement.

Le calendrier de **conservation**

Les données doivent être conservées uniquement le temps nécessaire aux fins pour lesquelles elles ont été collectées. Voici un exemple de calendrier que vous pouvez adapter.

Catégorie de données	Exemples	Durée de conservation	Raison
Données d'identité	Nom, date de naissance, NAS	5 ans après la relation	Exigences fiscales et légales
Données de contact	Adresse, téléphone, courriel	3 ans après dernier contact	Opérations de marketing
Données transactionnelles	Historique d'achats, factures	7 ans après transaction	Obligations comptables
Données d'emploi	CV, lettres, évaluations	2 ans après l'emploi	Réglementations du travail
Données de navigation	Logs, cookies	6 mois	Analyse comportementale
Vidéosurveillance	Enregistrements vidéo	1 mois	Sécurité des locaux

Finalité

Ne conserver que pour la durée nécessaire aux fins prévues.

Révision régulière

Revoir le calendrier pour rester conforme aux lois en vigueur.

Destruction sécurisée

Détruire ou anonymiser en fin de cycle pour éviter toute fuite.

Le registre des incidents

La Loi 25 impose de tenir un registre des incidents de confidentialité. Voici les éléments qu'il doit documenter — un modèle que vous pouvez reproduire dès aujourd'hui.

Date de l'incident Date exacte de découverte ou de survenance.	Type d'incident Accès non autorisé, perte, cyberattaque...	Données affectées Types de renseignements compromis.
Personnes concernées Nombre de personnes touchées.	Description Résumé des faits et premières observations.	Mesures prises Actions immédiates et stratégies de prévention.
Responsable Personne ou équipe en charge de la gestion.	Date de notification Quand les parties concernées ont été informées.	Notification à la CAI ? Indique si l'incident a été signalé à la Commission d'accès à l'information, comme requis dans certains cas.



Réflexe à adopter

Un incident présentant un « risque de préjudice sérieux » doit être consigné **et** notifié à la CAI ainsi qu'aux personnes concernées, dans les meilleurs délais.

Les procédures **essentielles**

Quatre procédures couvrent l'essentiel des situations courantes. Inutile de réinventer la roue : partez de modèles existants et adaptez-les à votre réalité.

Conservation, destruction & anonymisation

01

Encadre le cycle de vie des renseignements personnels, de la collecte à leur suppression sécurisée.

Demande d'accès & traitement des plaintes

02

Définit comment répondre à une personne qui souhaite consulter ou contester ses renseignements.

Désindexation & suppression

03

Encadre le droit à l'oubli : retrait et suppression des renseignements sur demande.

Gestion des incidents de sécurité

04

Décrit la réponse aux violations de renseignements, du signalement à la notification.

— POINTS CLÉS À CONSIDÉRER

- ✓ **Ne pas réinventer la roue** — utilisez des modèles éprouvés et adaptez-les.
- ✓ **Rôles & responsabilités** — précisez qui doit faire quoi, et quand.
- ✓ **Diffusion** — assurez-vous que la procédure est connue de toutes les parties prenantes.

Auto-évaluation de votre maturité

Cochez les éléments déjà en place dans votre entreprise, puis additionnez-les pour situer votre niveau de conformité.

☐ Responsable Loi 25 désigné

☐ Politique de confidentialité publiée

☐ Registre des incidents tenu

☐ Inventaire des renseignements personnels

☐ Procédure de destruction en place

☐ Employés sensibilisés

☐ ÉFVP réalisée pour les nouveaux projets

☐ Accès révoqués au départ des employés

— VOTRE SCORE

0 – 3

À structurer

Plusieurs écarts possibles : il est temps de poser les bases.

4 – 6

Bonne progression

Les fondations sont là ; quelques actions ciblées vous rapprochent.

7 – 8

Excellent niveau

Belle maturité — maintenez vos bonnes pratiques et révisiez-les.



Envie d'un portrait précis ?

Notre diagnostic préliminaire évalue votre niveau réel en moins de 30 minutes et vous remet une feuille de route priorisée. (Voir page suivante.)

04

PARTIE 4

Aller plus loin

Vous savez désormais ce que la loi attend de vous. La dernière étape — la plus simple — consiste à faire le point sur votre situation réelle et à prioriser vos actions.

12 Comment NB Solution vous accompagne

13 Votre diagnostic gratuit

Comment **NB Solution** vous accompagne

Nous transformons une obligation légale en avantage concurrentiel : une conformité solide, des outils prêts à l'emploi et une posture de cybersécurité renforcée.



Diagnostic Loi 25

Analyse de votre situation actuelle, identification des écarts et plan d'action priorisé.



Documentation

Politiques de confidentialité et de gouvernance, registres des incidents et des traitements, procédures, formulaires de consentement et gabarits ÉFVP.



Cybersécurité

Protection des accès, gestion des mots de passe, authentification multifacteur (MFA), sauvegardes et sensibilisation des employés.

✓ Cybersécurité

✓ Intégration Odoo

✓ Automatisation par l'IA

— OFFRE DÉCOUVERTE GRATUITE

Prêt à évaluer votre niveau de **conformité** ?

En moins de 30 minutes, nous réalisons un diagnostic préliminaire de votre situation et identifions vos actions prioritaires — sans engagement.

1

Analyse de votre situation actuelle

2

Identification des écarts

3

Feuille de route personnalisée



SCANNEZ POUR COMMENCER

Votre diagnostic préliminaire gratuit

Pointez l'appareil photo de votre téléphone vers le code, ou rendez-vous sur :

www.nbsolution.link/autodiagnostic



418-800-2030 · info@nbsolution.link



« La conformité à la Loi 25 n'est pas qu'une obligation légale : c'est un investissement dans la confiance de vos clients. »

NOS EXPERTISES

Cybersécurité & conformité Loi 25

Intégration Odoo

Automatisation par l'intelligence artificielle

NOUS JOINDRE

418-800-2030

info@nbsolution.link

www.nbsolution.link

20 Charest Ouest, bureau 102
Québec (QC) G1K 1X2, Canada