GUIDE SUR LA LOI 25

Adapté au commerce électronique

La Loi 25 a entraîné des changements importants pour les organisations et les entreprises. Le secteur du commerce électronique est particulièrement touché par ces nouvelles règles. Êtes-vous conformes aux règlementations déjà en vigueur depuis 2022 ? Êtes-vous préparé aux nouvelles modifications qui rentreront en vigueur le 23 septembre 2023 ?

Définition et rappel :

La Loi 25 a pour objectif de moderniser les dispositions législatives en matière de protection des renseignements personnels dans le secteur privé. En d'autres termes, la loi vise à mettre à jour les règles pour mieux protéger les données personnelles des individus dans les entreprises et organisations.

Clause de non-responsabilité

Bien que ce guide soit une introduction utile pour mieux comprendre et découvrir le paysage complexe de la Loi 25 tout en vous permettant d'accéder à des outils pertinents, il est important de noter qu'il ne peut en aucun cas se substituer à des conseils professionnels juridiques. La mise en conformité d'une organisation avec les nouvelles exigences de la Loi 25 est un processus spécifique à chaque organisation, il n'y a pas de modèle universel pour y parvenir.

En raison de ce qui a été mentionné précédemment, il est important d'utiliser les informations contenues dans ces documents avec précaution. Il est également important de noter que ces documents ne peuvent être considérés comme un avis juridique

En conséquence, PME MTL Centre-Ouest et l'Initiative eLog ne peuvent être tenus responsables des dommages directs ou indirects, des dommages exemplaires, des dommages accessoires ou particuliers, prévisibles ou non, liés à une réclamation résultant de l'utilisation des informations présentées dans ces documents.

Nous contacter : elog@pmemtl.com
Site Web : www.elogqc.ca

Liste de vérification - 10 points à retenir

1. Nommer une personne responsable de la protection des renseignements personnels et publier ses coordonnées sur le site Web de l'entreprise.
2. Avoir établi des politiques sur la sécurité des renseignements personnels que vous possédez et publier ces politiques sur votre site Web.
3. Ne recueillir que les informations nécessaires pour atteindre un objectif spécifique (demander le consentement pour cet objectif précis), et communiquer clairement cet objectif lors de la collecte des renseignements.
4. En cas d'incident de bris de confidentialité impliquant des renseignements personnels, il est exigé de prendre toutes les mesures nécessaires pour éviter que des incidents similaires ne se produisent à l'avenir. Dans ce cadre, il est requis de tenir un registre de ces incidents et, selon le degré d'importance de l'incident, d'informer la personne concernée ainsi que la Commission d'accès à l'information du Québec.
5. Il est exigé de respecter les nouvelles mesures d'encadrement du partage des données personnelles à des fins d'étude, de recherche, de statistiques ou dans le cadre d'une transaction commerciale.
6. Informer la Commission d'accès à l'information du Québec si vous avez l'intention de procéder à des vérifications d'identité en utilisant des mesures biométriques. *Les mesures biométriques sont des méthodes d'identification qui utilisent les caractéristiques biologiques d'une personne, telles que sa voix ou son visage, par exemple.*
7. Communiquer à votre clientèle si vous utilisez une technologie pour les identifier, les localiser ou les profiler, et communiquer votre politique de confidentialité.
8. S'il y a un transfert de données hors Québec, il faudra prendre en compte qu'un examen approfondi peut être nécessaire.
9. Prévoir par défaut les paramètres qui assurent le plus haut niveau de confidentialité du produit ou du service technologique offert au public.
10. Détruire les renseignements personnels que vous détenez dès que l'objectif pour lequel vous les avez collectés est atteint, à la suite du délai raisonnable prévu par la loi.

Nous contacter : elog@pmemtl.com
Site Web : www.elogqc.ca

Outils

- Exemple de politique de confidentialité adaptée au commerce électronique
- Exemple de procédures internes pour la protection des renseignements personnels
- Exemple – registre des incidents
- Exemple – gestion des demandes d'accès, des plaintes et des demandes de suppression
- Exemple – attestation de remise des biens

Note : vous pouvez créer un dossier avec tous les outils et modèles **adaptés à votre entreprise** dans vos fichiers.

Conseils et explications

1. Nommer une personne responsable de la protection des renseignements personnels

Que faut-il faire?

- Désigner la personne responsable, décrire son rôle et ses responsabilités (voir exemple de procédures internes) ;
- Définir / modifier le modèle de gouvernance en fonction des rôles et responsabilités ;
- Assurer la formation de la personne responsable ;
- Publier les coordonnées de la personne responsable publiquement (site Web) sur la page de la politique de confidentialité.

Note : Il est important de souligner que la formation de la personne responsable est importante pour combler l'écart potentiel de compétences entre la personne retenue et les compétences requises pour ces responsabilités.

2. Établir des politiques de confidentialité

La politique de confidentialité détaille ainsi :

- L'identité du responsable du traitement des données ;
- La nature des données collectées ;
- Le processus de rétention des données ;
- L'objectif de la collecte de données personnelles ;
- Le droit au retrait des personnes ;
- Qui a accès aux données et le processus de destruction ;
- La procédure de traitement d'un incident de confidentialité et les délais de notification d'un incident.

Voir un exemple de politique ici.

Nous contacter : elog@pmemtl.com
Site Web : www.elogqc.ca

Nous vous conseillons de créer une page pour la politique et d'intégrer un lien dans le pied de page de votre site web.

3. Inventaire des renseignements personnels de l'entreprise

Afin de savoir si les renseignements personnels de l'entreprise (que ce soit pour les employés, les clients, les fournisseurs, les sous-contractants, etc.) sont bien protégés, il est utile de faire un inventaire de ces derniers. Un exemple d'inventaire est proposé dans le modèle de procédures internes par type de renseignements et d'activité.

L'inventaire doit comprendre les informations suivantes :

- Les informations collectées (ex. Clients) et le type d'informations (civilité, sexe, identité, etc.)
- Où sont stockés les renseignements personnels
- Qui a accès aux renseignements personnels et dans quel contexte
- Quels sont les renseignements personnels transférés vers des tiers et s'ils sont transférés hors Québec

Faire cet exercice permettra d'effectuer une analyse d'impact pour évaluer les risques sur la protection des renseignements personnels et mettre en place des mesures pour les atténuer si nécessaire.

4. Collecte des renseignements personnels et consentement

Selon la loi, il ne faut recueillir que les informations nécessaires pour atteindre un objectif spécifique (et demander le consentement pour cet objectif précis). Il faut également communiquer clairement cet objectif lors de la collecte des renseignements.

Obtenir le consentement

Il est nécessaire d'obtenir le consentement dans les formulaires de contact, les avis clients ou la création d'un compte client pour vos objectifs (ex. marketing).

Pour cela, il peut être ajouté :

- Une case à cocher avec la mention « J'ai lu et j'accepte la politique de confidentialité » ;
- Une case à cocher : « en m'abonnant, j'accepte de recevoir des communications par courriel de la part de [nom de l'entreprise] à des fins publicitaires ».

Obtenir le consentement des témoins (cookies)

Shopify :
Si vous êtes sur Shopify, voici des outils qui pourraient être utilisés :

- Avada EU GDPR Cookie Consent : https://apps.shopify.com/avada-cookie-bar (application gratuite) ;
- Consentmo Conformité RGPD : https://apps.shopify.com/gdpr-backpack?locale=fr (application payante mais avec une portion gratuite).

- Cookiebot : https://www.cookiebot.com/ . Ce plugin utilise une technologie d'analyse en temps réel pour détecter les cookies et permettre aux utilisateurs de donner leur consentement (version gratuite limitée à 1 domaine, 1 langue sur le site et 50 sous-pages).

WooCommerce / WordPress :

- Cookie Notice & Compliance for GDPR / CCPA : https://en-ca.wordpress.org/plugins/cookie-notice/ . Permet de personnaliser les messages de consentement pour les cookies (application payante mais avec une portion gratuite selon le trafic sur le site Web) ;
- CookieYes | GDPR Cookie Consent & Compliance Notice : https://en-ca.wordpress.org/plugins/cookie-law-info/ . Permet également de personnaliser les messages de consentement (application payante mais avec une portion gratuite selon le trafic sur le site Web) ;
- Cookiebot : https://www.cookiebot.com/ . Ce plugin est un peu plus avancé que les deux précédents.

Infolettres

En plus du consentement pour l'inscription et la mention que l'objectif final est publicitaire, il faut que la personne puisse se désabonner facilement (lien dans l'infolettre).

Google Analytics

Si vous utilisez Google Analytics et que vous transférez des données vers Google, vous devez accepter les conditions de ventes de Google dans votre compte Google Analytics dans **Administration ---- Paramètres du comptes – accepter les conditions.**

5. Incident en lien avec un bris de confidentialité

Nous contacter : elog@pmemtl.com
Site Web : www.elogqc.ca

En cas d'incident de sécurité impliquant des renseignements personnels, les organisations doivent tenir un registre, et, selon le degré d'importance, en informer rapidement la Commission d'accès à l'information du Québec et les personnes concernées.

Voir un exemple de registre des incidents ici.

Il est important d'enquêter sur l'incident pour connaître la source et éviter que cela ne se reproduise.

6. Droit d'accès, de modification et de suppression des données

La Loi 25 donne aux personnes le droit d'accéder aux informations personnelles les concernant détenues par une entreprise, et de demander la correction ou la suppression de leurs données si elles sont inexactes, incomplètes ou obsolètes. Nous proposons des procédures et des registres dans le modèle correspondant.

7. Travailler avec des tiers

Les données fournies aux tiers (fournisseurs, sous-contractants) tombent aussi sous votre responsabilité. Il faut donc mettre en place des mesures d'atténuation et revoir vos contrats et ainsi :

- Interdire toute utilisation non convenue ;
- Permettre l'extraction de ses informations en cas de fin ou d'arrêt de contrat ;
- Destruire les informations à la fin du contrat ;
- Collaborer lors d'un incident de confidentialité (et de cybersécurité) ;
- Droit de vérification / audit / rapport de conformité (SOC 2 type 2).

RAPPEL - Clause de non-responsabilité

Bien que ce guide soit une introduction utile pour mieux comprendre et découvrir le paysage complexe de la Loi 25 tout en vous permettant d'accéder à des outils pertinents, il est important de noter qu'il ne peut en aucun cas se substituer à des conseils professionnels juridiques. La mise en conformité d'une organisation avec les nouvelles exigences de la Loi 25 est un processus spécifique à chaque organisation, il n'y a pas de modèle universel pour y parvenir.

En raison de ce qui a été mentionné précédemment, il est important d'utiliser les informations contenues dans ces documents avec précaution. Il est également important de noter que ces documents ne peuvent être considérés comme un avis juridique

En conséquence, PME MTL Centre-Ouest et l'Initiative eLog ne peuvent être tenus responsables des dommages directs ou indirects, des dommages exemplaires, des dommages accessoires ou particuliers, prévisibles ou non, liés à une réclamation résultant de l'utilisation des informations présentées dans ces documents.

Références

Nous contacter : elog@pmemtl.com
Site Web : www.elogqc.ca

Pour réaliser ce guide, nous avons utilisé et combiné plusieurs outils, certains internes et d'autres publics, notamment :

- Mes procédures
- Le guide sur l'utilisation de la Loi 25 de Cybereco.
- In-Sec-M : formulaire de diagnostic (coût de 60 $) et formations (payantes) existantes : https://insecm.ca/

Nous contacter : elog@pmemtl.com
Site Web : www.elogqc.ca