Politique sur la gouvernance des renseignements personnels (confidentialité)

1. Le préambule

Dans l'exercice de gestion **Villa Toyota** doit recueillir, traiter et communiquer des renseignements jugés personnels. Dans ce cadre, **Villa Toyota** désire mettre en place, en respect de la *Loi sur la protection des renseignements personnels dans le secteur privé, chapitre p-39.1,* les processus, les méthodes, les règlements, les politiques pour assurer que le recueil, le traitement, la communication, la protection et la destruction des renseignements personnels soient conformes à la législation en vigueur dans ce domaine, et ultimement, assurer l'absence de tout incident de confidentialité et dans le cas contraire avoir en place les processus nécessaires pour minimiser ou éliminer les préjudices sérieux.

2. Les objectifs de la politique

La présente politique vise les objectifs suivants :

- Respecter la *Loi sur la protection des renseignements personnels dans le secteur privé, chapitre p-39.1 ;*
- Protéger les renseignements personnels présents ;
- Réagir avec efficacité et démontrer la diligence de (nom de l'organisation) ;
- Comprendre ce qu'est un renseignement personnel ;
- Définir clairement les responsabilités et les obligations de chaque intervenant dans l'organisation ;
- Avoir en place les politiques et pratiques pour protéger les renseignements personnels détenus par (nom de l'organisation);
- Établir les actions à entreprendre dans le cas d'un risque d'incident de confidentialité sans préjudice sérieux ;

- Établir les actions à entreprendre dans le cas d'un incident de confidentialité avec un risque de préjudicie sérieux ;
- Établir les modes de destructions sécuritaires de renseignements personnels ;
- Établir les règles de conservation des renseignements personnels.

3. L'engagement de l'organisation

(Nom de l'organisation) s'engage à assurer la protection des renseignements personnels qu'elle détient, acquiert, traite, transmet et détruit.

4. Le rôle et les responsabilités des membres du personnel et des cadres

Chaque membre du personnel et cadre ont la responsabilité de protéger et d'utiliser à bon escient les renseignements personnels accessibles dans le cadre du travail tout au long du cycle de vie des renseignements personnels.

En aucun temps, le membre du personnel ou le cadre ne recueillera, ne consultera, ne transmettra ou ne détruira des renseignements personnels sans avoir au préalable reçu la permission du responsable de la protection des renseignements personnels ou en cas d'absence, de son remplaçant.

Le non-respect de cette obligation pourrait engager un processus disciplinaire pouvant se traduire par un congédiement.

5. Le rôle et les responsabilités du responsable de la protection des renseignements personnels tout au long du cycle de vie des renseignements personnels

La personne responsable de la protection des renseignements personnels doit :

- Définir son rôle et ses responsabilités au sein d'une politique ;
- Faire l'inventaire des renseignements personnels détenus et évaluer leur sensibilité ;
- Mettre en place des mesures pour prévenir ou limiter les conséquences d'un incident de confidentialité impliquant un renseignement personnel ;

- Réaliser les évaluations des facteurs relatifs à la vie privée (ÉFVP). L'ÉFVP est un processus qui sert à déterminer l'incidence que pourrait avoir un programme ou un service sur la vie privée d'une personne ;
- Sensibiliser et former le personnel de l'entreprise ;
- Assurer la gestion des incidents de confidentialité et tenir un registre de ces derniers ;
- Connaître la nature des renseignements personnels que (nom de l'organisation) possède ;
- Détenir, traiter et communiquer les renseignements personnels selon les règles édictées par la Loi ;
- Savoir qui peut avoir accès à ces renseignements personnels et pour quels motifs ;
- S'assurer que les renseignements personnels dont les personnes ont accès sont exigés dans le cadre de leurs fonctions ;
- Produire et mettre en place des politiques et des pratiques qui encadrent la gouvernance des renseignements personnels ;
- Appliquer ou faire appliquer les politiques et pratiques en matière de renseignements personnels.

6. La collecte de renseignements personnels

La collecte de renseignements personnels doit se faire en suivant les 3 règles suivantes :

- La règle du consentement ;
- La règle de l'intérêt sérieux et légitime et de la nécessité ;
- La règle de la cueillette directe.

7. La sécurité des renseignements personnels recueillis par la technologie de l'information

7.1 La technologie de l'information

Villa Toyota utilise les technologies de l'information pour supporter ses opérations. Les renseignements personnels recueillis servent à offrir des services conformes aux attentes des personnes concernées et à la déclaration des services de (nom de l'organisation).

Tous les renseignements personnels qui sont collectés sont conservés dans un environnement sécurisé rencontrant les obligations de la Loi.

7.2 Les employés

Tous les employés de **Villa Toyota** ont l'obligation de suivre les indications prévues dans la présente politique et d'agir en tout temps pour préserver la sécurité des renseignements personnels détenus et traités par **Villa Toyota**. Comme prévu aux présentes **Villa Toyota** doit mettre en place des mesures de sécurité et de gestion des accès adéquates, utiles et nécessaires selon le niveau de sensibilité des renseignements personnels recueillis et traités par la technologie de l'information.

7.3 L'accès aux renseignements personnels recueillis par la technologie de l'information

L'accès aux renseignements personnels obtenus par la technologie de l'information sera limité aux seules personnes ayant la qualité pour les recevoir au sein de l'organisation lorsque ces renseignements sont nécessaires à l'exercice de leurs fonctions.

8. L'utilisation des renseignements personnels

8.1 L'utilisation

Les renseignements personnels ne peuvent être utilisés que pour la fin pour laquelle ils ont été collectés. Dans le cas où les renseignements personnels seraient utilisés pour une autre fin, l'autorisation de la personne concernée devra être donnée avant l'utilisation des renseignements personnels.

Comme il est prévu à la Loi, la collecte des renseignements personnels donne l'autorisation de la part de la personne concernée d'utiliser les renseignements collectés. Spécifiquement, les limites de l'utilisation des renseignements personnels sont les suivantes :

- Limiter l'accès aux renseignements personnels aux seules personnes ayant la qualité pour les recevoir au sein de l'organisation lorsque ces renseignements sont nécessaires à l'exercice de leurs fonctions ;

- Limiter l'utilisation des renseignements personnels : à moins d'une exception prévue par la loi, le consentement doit être obtenu de la personne concernée pour utiliser ses renseignements une fois l'objet du dossier accompli.

8.2 La sécurité lors de l'utilisation

Pendant l'utilisation des renseignements personnels, la personne qui en fait usage doit obligatoirement en assurer la protection. La personne doit, sans s'y restreindre.

- Ne pas donner accès aux renseignements personnels à une personne qui n'y est pas autorisée ;

- Dans le cas où la personne qui utilise les renseignements personnels quitte temporairement son espace de travail, les renseignements personnels doivent être disposés de manière à ne pas être à la vue des passants :

    - Les renseignements personnels doivent être rangés dans un classeur ou tiroir barré ;

    - L'écran de l'ordinateur doit être verrouillé.

- S'assurer que les renseignements personnels ne puissent être vus de l'extérieur de son poste de travail ou de son bureau ;

- Lors de discussions traitant de renseignements personnels, celles-ci doivent se faire dans un lieu privé où la discussion ne peut être entendue par les personnes qui n'ont pas l'autorisation d'y avoir accès.

9. La communication de renseignements personnels

9.1 Le consentement à la communication

Avant toute communication, qu'elle soit verbale ou écrite et par tous les moyen, téléphone, courriel, texto, lettre, rapport, site Web ou, etc., le consentement de la personne concernée est nécessaire sauf dans les cas prévus à la Loi.

Spécifiquement, les obligations suivantes doivent être respectées :

- Obtenir le consentement des personnes concernées pour communiquer leurs renseignements à un tiers (ex. : assureur ou prestataire de services), à moins d'une exception prévue par la Loi ;

- Respecter la règle du consentement (voir article 7.1) ;

- Respecter les obligations prévues par la Loi lorsqu'elle communique des renseignements personnels sans le consentement de la personne concernée ;

- Respecter les obligations particulières applicables à la communication de renseignements personnels à l'extérieur du Québec.

L'autorisation de collecter et d'utiliser les renseignements personnels ne permet pas la communication à un tiers des renseignements en question.

La personne concernée devra remplir et signer le formulaire *pour le consentement à la communication.*

10. Le traitement des plaintes relatives à la protection des renseignements personnels

10.1 Le traitement des plaintes

Le traitement adéquat, uniforme et diligent des plaintes est une priorité chez (nom de l'organisation). Toute personne insatisfaite du processus de collecte, d'utilisation, de communication ou de destruction de renseignements personnels peut déposer une plainte à la personne responsable de la protection des renseignements personnels.

10.2 Le processus de traitement d'une plainte.

Dans le cas où une plainte est déposée, le responsable de la protection des renseignements personnels doit suivre les étapes prévues à la *Procédure de traitement d'une plainte*. Il bénéficie de 30 jours pour le faire. Les étapes suivantes devront être suivies :

a) Réception de la plainte

b) Analyse de la recevabilité

c) Si la plainte est non recevable

- Lettre à la personne plaignante et arrêt du processus

d) Si la plainte est recevable

- Lettre à la personne plaignante et enquête

e) Enquête

f) Résultat de l'enquête

g) Avis écrit à la personne plaignante sur le résultat de l'enquête

h) Mise en place des solutions

La personne responsable prendra toutes les actions pour protéger au maximum les renseignements personnels détenus, traités et communiqués.

10.3 Les mesures de sécurité

La personne responsable devra mettre en place des mesures de sécurité propres à assurer la protection des renseignements personnels collectés, utilisés, communiqués, conservés ou détruits.

Ces mesures sont raisonnables compte tenu notamment de la sensibilité, de la finalité, de la quantité, de la répartition et du support des renseignements personnels.

11. La conservation des renseignements personnels

Le responsable de la protection des renseignements personnels verra à la conservation des renseignements personnels. La conservation consiste en la période de temps pendant laquelle sont conservés les renseignements personnels, sous quelque forme que ce soit, et ce, peu importe que les renseignements soient activement utilisés ou non.

11.1 Les règles de conservation

Il s'agit spécifiquement :

- **Assurer la mise à jour et l'exactitude des** renseignements personnels détenus au moment où ils sont utilisés pour une décision relative à la personne concernée ;

- **Mettre en place et respecter les mesures nécessaires pour assurer la sécurité des renseignements personnels ;**

- Conserver les renseignements personnels jusqu'à l'atteinte de la finalité pour laquelle ils ont été collectés ou selon les modalités déterminées par une loi ;

- Conserver les renseignements personnels dans un endroit sécuritaire et prévu à cette fin ;

- Permettre l'utilisation des renseignements personnels lorsque la finalité pour laquelle ils ont été collectés est accomplie, qu'avec le consentement de la personne concernée, sous réserve du délai prévu par la loi ou par un calendrier de conservation établi par règlement du gouvernement.

11.2 La fin de la durée de conservation

À la fin de la durée de conservation des renseignements personnels, soit à l'arrivée de la finalité pour laquelle ils ont été collectés, (nom de l'organisation) s'assurera :

- De les détruire de manière sécuritaire et comme prévu à la présente politique ;

Ou

- De les anonymiser (c'est-à-dire qu'ils ne permettent plus d'identifier la personne concernée ni d'établir un lien entre la personne concernée et les renseignements personnels) et ce de manière irréversible dans le but de les utiliser à des fins sérieuses et légitimes.

11.3 Le temps de conservation

Le temps de conservation est la durée nécessaire à la réalisation des fins pour lesquelles il a été demandé ou celui prévu au document sur le *temps de conservation des renseignements personnels* ou celui prévu à une loi en vigueur.

12. Les règles de destruction des renseignements personnels

Le responsable de la protection des renseignements personnels doit s'assurer que la destruction des renseignements personnels se fasse de manière sécuritaire. De plus, si l'organisation désire garder les renseignements personnels, le responsable de la protection des renseignements personnels devra en assurer l'anonymisation et l'utilisation à des fins sérieuses et légitimes.

12.1 Le moment de la destruction

Le responsable de la protection des renseignements personnels devra faire en sorte et prendre les mesures nécessaires lorsque la finalité pour laquelle les renseignements personnels ont été collectés est accomplie, sous réserve du délai prévu par la loi ou par un calendrier de conservation établi par règlement du gouvernement (ex. pour des obligations fiscales), qu'ils soient détruits.

12.2 Les méthodes de destruction

Une méthode de destruction est un processus qui permet de détruire de manière permanente et irréversible des renseignements personnels. Il peut s'agir de déchiqueter, formater, réécrire, destruction physique, broyage, démagnétisation, écrasement d'information. Les pratiques sont prévues au document *Méthode de destruction de renseignements personnels*.

12.3 Les méthodes d'anonymisation

Une méthode d'anonymisation est un processus irréversible par lequel les renseignements personnels sont traités de manière à rendre impossible l'identification directe ou indirecte de la personne concernée.

12.4 L'application de la politique

Le responsable de la protection des renseignements personnels a la responsabilité d'interpréter et d'appliquer la politique.

12.5 Révision de la politique

La présente politique sera révisée tous les 3 ans.

12.6 La date d'entrée en vigueur

La politique entrera en vigueur le 22 septembre 2023.